Uso de herramientas informáticas para descubrir vulnerabilidades en las redes wifi domesticas

Anggie Katherin Ovalle Velez

Trabajo de grado presentado para optar al título de especialista en seguridad de la información

Asesor: MSc. Nelson Augusto Forero Páez, PhD (c)

Universidad Católica de Colombia

Facultad de Ingeniería

Especialización en Seguridad de la Información

Bogotá D.C., Colombia

2019

Dedicatoria

A mi mamá: Maria Paulina Velez, a mi abuela: Maria del Carmen Labrador de Velez y a mi Gato Pepe, los quiero y adoro mucho

Agradecimientos

Quiero agradecer a las personas que me ayudaron en su participación a sacar adelante este proyecto en su parte práctica, a mi tutora de ante proyecto Ing. Sandra Bernate, mi tutor de proyecto Ing. Nelson Forero, a mi mama, abuela y mi gato, gracias a todos por su apoyo, les estoy agradecida en el alma.

TABLA DE CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

RESUMEN

Este proyecto trabaja con base la seguridad de las redes wifi-hogareñas, el objetivo de este es el diseño e implementación de un manual para el usuario final, que le permita detectar las vulnerabilidades presentes en la red, para esto, el manual cuneta con 3 unidades: 1) Vulneración de la red Wifi, se busca la violación de la seguridad de la red wifi (ruptura de la clave de acceso a la red), 2) Escaneo de red, su objetivo es la identificación de dispositivos conectados a la red, carpetas compartidas, puertos y el análisis del tráfico de la red y 3) Escaneo de Vulnerabilidades, el cual le permitirá al usuario identificar las vulnerabilidades presentes en los dispositivos conectados a la red, informándole acerca de los peligros que estas falencias pueden causarle a la seguridad de la información, los manuales descritos usan software gratuito para su uso final. Para su aplicación inicial se usó una muestra poblacional de 10 personas, las cuales aplicaron el manual, compartieron sus resultados y se les fue retroalimentado acerca de las novedades encontradas en sus redes, para ellos, este manual les ayudo a identificar las vulnerabilidades presentes en sus redes y así tomar las medidas necesarias para contrarrestarlos.

Palabras clave: Vulnerabilidades, red Wifi, hogar, ciberseguridad, análisis de riesgo, información.

ABSTRACT

This project works based on the security of Wi-Fi home networks, the objective of this is the design and implementation of a manual for the end user, which allows him to detect the vulnerabilities present in the network, for this, the gutter manual with 3 units: 1) Wi-Fi network violation, the violation of the security of the Wi-Fi network is sought (breaking the access key to the network), 2) Network scanning, its objective is the identification of devices connected to the network , shared folders, ports and the analysis of network traffic and 3) Vulnerability Scan, which will allow the user to identify the vulnerabilities present in the devices connected to the network, informing him about the dangers that these failures can cause to the Information security, the manuals described use free software for final use. For their initial application a population sample of 10 people was used, who applied the manual, shared their results and were given feedback about the novelties found in their networks, for them, this manual helped them identify the vulnerabilities present in their networks and thus take the necessary measures to counteract them.

Keywords: Vulnerabilities, Wi-Fi network, home, cybersecurity, risk analysis, information.

I. INTRODUCCIÓN

Con el rápido crecimiento de las comunicaciones y el desarrollo de nuevas tecnologías que apuntan a que tengamos una vida más cómoda ajustándose a nuestras necesidades, y su implicación a que estemos conectados a diario a la red usando desde el celular inteligente hasta asistentes de voz, pasando por relojes inteligentes, computadores, cámaras IP, entre otros. ¿Qué tienen en común estos elementos? que requieren estar conectados a internet para sacar provecho de sus múltiples funcionalidades y su puerta de salida es en muchos casos el Router de la red al que están conectados, una mala configuración de este dispositivo puede poner a merced de los atacantes la seguridad de los equipos tecnológicos conectados a la red. Cabe resaltar que estos dispositivos tiene un mecanismo de defensa, pero si no está configurado de forma correcta o por temas de sistema operativo tiene vulnerabilidades que no se han parchado con las actualizaciones periódicas de los fabricantes, al igual que la falta de conocimiento por parte del usuario en seguridad al momento de navegar por internet, obtenemos un escenario perfecto para los ciberdelincuentes quienes no pierden oportunidades para aprovechar la oportunidad y obtener información valiosa de la víctima para sacar beneficios, estos y más casos son publicados por Kaspersky en su Blog de noticias [1].

En las empresas los administradores de red establecen estrategias que minimizan los riesgos que pueden afectar la seguridad de la información, así como la estabilidad de los dispositivos, sin embargo, en las redes hogareñas, el desconocimiento de los usuarios finales los deja expuestos a las diversas amenazas.

Con base en lo anterior se propone responder a la pregunta ¿Cómo atacar una red hogareña para identificar brechas de seguridad de la información sin tener conocimiento del tema?, por lo que se establece como metodología de trabajo en cuatro fases cuyo resultado final será la obtención de una manual para usuario final de implementación fácil, que permita detectar las falencias de su red, el cual abarca desde el Router hasta los diferentes dispositivos conectados, realizando un inventario de los dispositivos que se encuentran conectados, búsqueda de vulnerabilidades y recomendaciones a seguir, para reducir los riesgos y amenazas de seguridad.

II. GENERALIDADES

A. Línea de Investigación

Este proyecto está enfocado en la línea de investigación de Software inteligente y convergencia tecnológica avalada por la Universidad Católica de Colombia.

B. Planteamiento del Problema

El desarrollo tecnológico ha permitido mayor acceso a los diferentes dispositivos, los cuales han incrementado las conexiones a internet tanto en empresas como hogares, según lo que indico el Ministro de las TIC David Luna durante el congreso Internacional de TIC Andicon 2017 que se llevó a cabo en la ciudad de Cartagena para el año 2017, la conectividad en hogares había aumentado el 64% [2], de forma proporcional han aumentado los ataques cibernéticos a nivel nacional e internacional, en el 2018 Kaspersky, compañía internacional dedicada a la investigación y desarrollos en seguridad, informo en su blog que en Americe Latina aumento un 60% los ciberataques, los cuales la mayoría están enfocadas al robo de dinero por medio de correos fraudulentos y vectores offline (como por ejemplo memorias USB) [3].

Las redes y equipos domésticos posiblemente son los más propensos a ataques desarrollados por delincuentes cibernéticos, debido a las amenazas que circulan no solo en la red si no en sus equipos, ya que estos pueden no protegerse de manera adecuada, llegando a ser altamente riesgosos, poniendo en peligro tanto la información que almacenan, así como la seguridad y estabilidad de los equipos (en caso de tener conexión a la red) que están dentro de la misma, aprovechándose de las vulnerabilidades del software, para robar, dañar o secuestrar información, también tomar el control de los equipos de forma remota sin que el usuario sepa lo que está sucediendo.

E. Antecedentes del problema

Con el acelerado desarrollo que han presentado las TIC en los últimos años, avanzan también los ciberataques los cuales son cada vez más estructurados y con una cobertura más amplia. De acuerdo con el informe presentado en Blog Kaspersky Lab Daily [3], para 2018, Colombia se posicionó en el puesto No. 10 de países latinoamericanos afectados por el phishing durante los primeros 7 meses de ese año como se puede observar en la

Ilustración *1*, indicando un aumento del 14%.

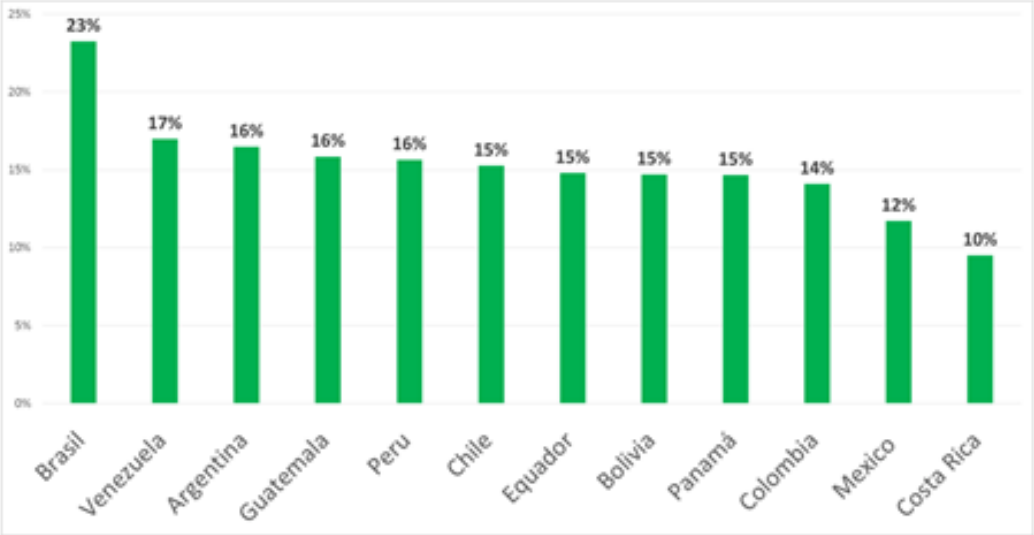


Ilustración 1: Ranking de países latinoamericanos afectados por phishing durante los primeros 7 meses de 2018

Tomado de: Kaspersly Lab Daily *[3]*

Una de las temporadas en las que más ataques de este tipo se presentan es en el "Black Friday" en donde aumenta el phishing casi más de 4 veces que en un día normal ya que la táctica que se usa para hacer caer a las victimas es sencilla, correos masivos con atractivas ofertas de productos, la mayoría tecnológicos, que con el simple hecho de dar clic sobre algún vínculo del correo, este redireccionara a la víctima a sitios falsos cuyo objetivo es capturar la información crediticia del usuario [3].

Así mismo, el uso de IoT, los asistentes para el hogar, como en el caso de los Apple HomePod, Amazon Echo, Google Home que poco a poco se están apoderando de las casas, a pesar de la gran inversión en seguridad en éste tipo de dispositivos, siguen siendo vulnerables como lo informa Hervé Lambert Consumer Global Operations Manager de Panda Security [4] "A priori, no se trata de ningún error por parte de sus desarrolladores. Lo que ocurre cada vez que el uso de una tecnología se convierte o va a convertirse en masivo es que los ciberdelincuentes vuelcan todos sus esfuerzos en encontrar vulnerabilidades. Así, consiguen sacar rendimientos económicos en forma de robos y extorsiones"

Con respecto a las redes Wifi, no todas son 100% confiables, pero se puede implementar la actualización de los routers, cambio de clave de la red cuando se note que su rendimiento con respecto a la velocidad de navegación baje sin razón aparente, esto último como recomendación por parte de Microsoft, el cual, en abril del presente año, ellos afirmaron que [5] "Si una contraseña no ha sido robada no hay necesidad de cambiarla. Y si hay evidencia de que ha sido robada, hay que actuar de inmediato, sin esperar a que caduque" y que su conexión sea segura [6], al menos que el protocolo implementado para la seguridad no sea sencillo de vulnerar como el caso del protocolo WEP el cual tiene bastantes huecos de seguridad permitiendo su fácil rompimiento, cabe resaltar que aun en la actualidad hay routers que dentro de sus protocolos de configuración de Wifi existe este [7].

Para este 2019 las redes sociales y el IoT serán los objetivos de los delincuentes para cometer y expandir sus delitos, sacando provecho de las personas que por motivos varios no tienen las medidas básicas para su protección, y ya sea por desconocimiento o negligencia caen en su red, sus ataques varían desde uso de vínculos o software malintencionado hasta ingeniería social [8].

Adicional, en el año 2017 se desarrolló en la Universidad Católica un trabajo de proyecto de grado titulado "Protocolos para la mitigación de ciberataques en el hogar. Caso de estudio: estratos 3 y 4 de la ciudad de Bogotá" [9] el cual consistía en realizar ataques a redes Wifi escogidos previamente y ya dentro de esta, escanear la red para buscar vulnerabilidades, cuyo resultado se les compartía a los participantes, dándoles consejos para que se protejan mas no deja para un manual para poder ejecutar un auto análisis para así determinar el nivel de seguridad .

F. Pregunta de investigación

¿Cómo identificar brechas de seguridad de la información en una red hogareña para sin tener conocimientos específicos de seguridad en las redes?

G. Variables del problema

Vulnerabilidades: al diseñar la red se busca reducir el número de vulnerabilidades halladas, con

base en la implementación del manual a desarrollar.

Riesgos: reducir el riego al que se expone la seguridad de la información, a través de la implementación de las recomendaciones establecidas en el manual.

C. Justificación

La predicción para este año en curso (2019) en temas de seguridad apunta a las vulnerabilidades hacia el ataque a los dispositivos del IoT (Internet of Things, conocido en español como internet de las cosas) y routers, lo cual informo Avast en su blog [10], en donde anuncia que para el 2020 abra un promedio de 38.500 millones de dispositivos conectados a internet, esta categoría aumenta drásticamente ya que "una persona habitualmente solo tiene un equipo portátil y un teléfono móvil, también tiene varios dispositivos conectados en su casa, desde el timbre de la puerta a dispositivos de entretenimiento y la seguridad de su hogar." [10], lastimosamente esta área se afecta debido a que "frecuentemente la seguridad es un concepto que se deja para el final en el proceso de fabricación de estos dispositivos.

Aunque muchos de los dispositivos inteligentes de las marcas más populares cuentan con una seguridad integrada razonable, algunos desarrolladores ahorran en seguridad para mantener precios asequibles para los consumidores, un error teniendo en cuenta que un hogar inteligente será solo tan seguro como lo sea su eslabón más débil." [11], como por ejemplo, IoT usa el protocolo MQTT el cual permite la interconexión y el control de dispositivos domésticos inteligentes, el cual se puede configurar a través de un pequeño servidor que puede ser un PC o una Raspberry Pi, y desde allí centralizar la administración de estos, pero una mala configuración puede poner en grave riesgo la seguridad y como plus si éste está público, ya que le permitiría conectarse a él desde cualquier lugar. Como se puede observar en la Ilustración 2, en el mundo hay alrededor de 49.000 servidores de MQTT de los cuales un 32.888 de estos se encuentran sin una contraseña. [11]

Ilustración 2: Servidores MQTT Públicos

Tomado de: Avast Blog *[11]*

Con respecto a los routers, cualquier hogar con internet posee este dispositivo al cual van conectados diferentes equipos tecnológicos con tarjeta de red como teléfonos, portátiles, televisores inteligentes, etc. Los cuales según Avast [10]: el 60% de los usuarios de estos dispositivos en el mundo "o bien nunca se han conectado a su router o nunca han actualizado el firmware del router, dejándolo potencialmente vulnerable a ataques bastante simples." Y esto se debe a que "una vez que el proveedor de internet ha instalado el router, la mayoría de las personas nunca vuelven a pensar en él, a no ser que experimenten fallos en la señal de internet." Los cuales pueden ser explotados para ejecutar dentro de la red código malicioso o simplemente espiar a los usuarios dentro de esta, lo cual es de vital importancia proteger nuestro router ya que es la puerta de entrada de nuestra red.

III. OBJETIVOS

E. Objetivo general

Diseñar un manual de ataque para redes hogareñas que permita a los propietarios de éstas identificar las vulnerabilidades presentes en su red y así reducir los riesgos de la información.

F. Objetivos específicos

- Establecer buenas prácticas para la configuración de la red con el fin de minimizar los riesgos.
- Probar en la red propia el manual de ataque diseñada para validar su consistencia.
- Diseñar el manual de ataque que será aplicada en las redes domésticas para identificar vulnerabilidades

IV. MARCOS DE REFERENCIA

A. Marco conceptual

A lo largo de este trabajo se irán mencionando términos que van asociados a la **ciberseguridad** (“práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos” [12]) y al **cibercrimen** (“actores individuales o grupos que dirigen ataques a sistemas para obtener ganancias financieras” [12]), los cuales para una persona que no tiene conocimientos a nivel informático le será confuso como por ejemplo el termino **virus** que para este contexto significa un “programa que agrega su código a otros programas para infectarlos y poder controlarlos cuando se los ejecuta. Esta definición simple permite identificar la acción principal de cualquier virus: la infección.” [13], también llamado **malware** (“Cualquier programa, documento o mensaje, susceptible de causar perjuicios a los usuarios de sistemas informáticos. MALicious softWARE.” [14]). Por lo general, los virus se aprovechan de las **vulnerabilidades** o debilidades existentes en los **sistemas operativos** (“Conjunto de programas fundamentales sin los cuales no sería posible hacer funcionar el ordenador con los programas de aplicación que se desee utilizar.” [15]) o aplicaciones que en su mayoría no tienen sus actualizaciones al día (también llamados **parches de seguridad** que se definen como el “conjunto de ficheros adicionales al software base de una herramienta o programa informático, que sirven para solucionar sus posibles carencias, vulnerabilidades, o defectos de funcionamiento.” [14]), el cual “ puede ser explotado por marcadores de software maliciosos para penetrar […] y dañar su integridad. […] ocasionando fallas de operaciones y en las aplicaciones instaladas.” [13].

Estas vulnerabilidades se pueden explotar por diferentes medios, como ejemplo, por medio de los **rootkit** (“programa o conjunto de aplicaciones desarrollados para ocultar los rastros de un intruso o software malicioso en el sistema operativo […] Muchos rootkits instalan sus propios controladores y servicios en el sistema operativo.” [13]), **troyanos** el cual “en sentido estricto, […] no es un virus, aunque se considere como tal. Realmente se trata de un programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario afectado [14], **ransomware** (ver Ilustración 3) cuyo propósito es infectar y encriptar la información del computador de su víctima y exigir, por

medio de mensajes emergentes [16], el pago de la recuperación de los archivos encriptados por medio de **Bitcoins** ("la definición de Bitcoin es muy sencilla, pues como tal es una moneda, como el euro o el dólar estadounidense, que sirve para intercambiar bienes y servicios. Sin embargo, a diferencia de otras monedas, Bitcoin es una divisa electrónica que presenta novedosas características y destaca por su eficiencia, seguridad y facilidad de intercambio" [17]). Algunos virus usan la técnica de **puerta trasera** que hace una apertura, por lo general a través del firewall "la cual es posible controlar el sistema afectado, sin conocimiento por parte del usuario." [14], a esta modalidad se le conoce también como **bot** ("Contracción de la palabra robot. Es un programa que permite que el sistema sea controlado remotamente sin el conocimiento ni consentimiento del usuario." [14])

Ilustración 3: Malware llamado WannaCrypt (de la familia de los ransomware) que infecto en el 2017 alrededor de 45.000 computadores a nivel mundial.

Tomado de: pbs.org *[18]*

Pero también hay amenazas que nos asechan con el simple hecho de navegar por la web como es el caso del **Trackware** que es un "programa que realiza el seguimiento de las acciones que realiza el usuario mientras navega por Internet (páginas visitadas, banners que pulsa, etc.) y crea un perfil que utiliza con fines publicitarios." [14], los **Adware** (ver Ilustración 4) que son "programas que muestran publicidad utilizando cualquier tipo de medio, por ejemplo: ventanas emergentes, banners, cambios en la página de inicio o de búsqueda del navegador, etc. Puede instalarse con el consentimiento del usuario y su plena conciencia, pero en ocasiones no es así. Lo mismo ocurre con el conocimiento o falta de este acerca de sus funciones" [14] estos en su mayoría son molestos cuando aparecen mientras se está navegando, pero otros con publicidad engañosa, atraen a la víctima haciéndole creer que gano un premio para obtener de él su información.

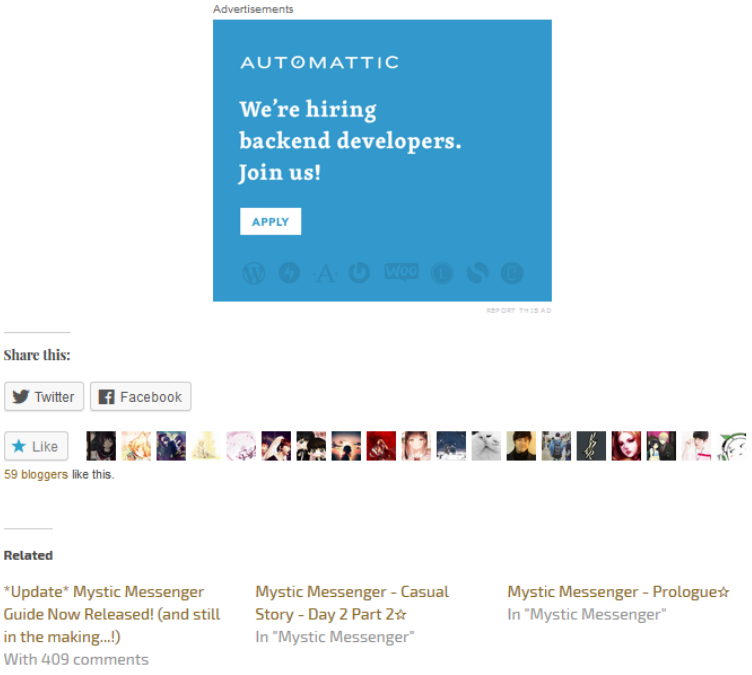


Ilustración 4: Ejemplo de Adware.

Tomado de: otomedreamworld.wordpress.com

También a través de la web nos podemos topar con **troyanos bancarios** cuya finalidad es "robar información confidencial a los clientes de banca y/o plataformas de pago online." [14], correo basura o **spam** ("Es correo electrónico no solicitado, normalmente con contenido publicitario, que

se envía de forma masiva. Este tipo de mensajes pueden causar graves molestias y provocar pérdidas de tiempo y recursos." [14]) el cual si no se sabe tratar puede generar al computador que sea víctima de **Spammer** ("Programa que permite el envío masivo de mensajes de correo electrónico con contenido publicitario y la consiguiente recepción masiva de éstos. Puede ser también empleado para el envío masivo de amenazas tales como gusanos y troyanos." [14]) o en el peor de los casos caer en un caso de **phishing** el cual "consiste en el envío masivo de mensajes que, aparentando provenir de fuentes fiables, intentan conseguir que el usuario proporcione datos confidenciales. El caso más típico de phishing es el envío de correos electrónicos que se hacen pasar por procedentes de una entidad bancaria online, para conseguir que el usuario introduzca sus contraseñas en una página web falseada." [14]

Pero no todo es malo, ya que con una debida protección no se correrá con los riesgos anteriormente mencionados, como, por ejemplo, tener instaladas las correspondientes actualizaciones de los programas y sistema operativo que se esté usando, un buen **antivirus** los cuales son "programas que permiten analizar la memoria, las unidades de disco y otros elementos de un ordenador, en busca de virus." [14] y para reforzar su efectividad combinarlo con un **antispyware** ("un tipo de herramienta capaz de detectar y erradicar de tu PC los programas espía." [19]) con una buena configuración del **FirreWall** ("Es una barrera o protección que permite a un sistema salvaguardar la información al acceder a otras redes, como por ejemplo Internet." [14]), también para proteger los archivos que se usan se puede usar el recurso de **Backup** ("Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados." [20]) , también con programas de **sniffer** que "monitoriza la información que circula por la red con el objeto de capturar información." [20] esto para analizar el tráfico y poder detectar anomalías y para valorar el estado de los equipos, hacer un análisis de vulnerabilidades a través de software especializado para este fin

B. Marco teórico

A diario se producen miles de ataques y descubrimientos de vulnerabilidades que no solo afectan a los empresarios si no a las personas que usan la tecnología para su distracción, la cual

implementan en su vida diaria por medio de IoT, como por ejemplo la última vulnerabilidad encontrada en la aplicación de chat WhatsApp en el mes de abril del 2019 en la cual la compañía informo que "grupo de hackers halló una falla de seguridad […] y la usó para instalar un programa espía en un número aún sin determinar de teléfonos […] mediante una llamada al número en cuestión a través de la aplicación" [21], lo cual permitió que se pudiera acceder a los datos que el dispositivo infectado contenía.

El riesgo más alto al que están expuestos los usuarios, son las vulnerabilidades de los dispositivos IoT, cuya finalidad es hacer la vida más cómoda y que estos de forma sencilla se puedan manipular desde la red, en la Ilustración 5, podemos observar que hay muchos dispositivos creados por diferentes empresas que ofrecen múltiples servicios, desde una cámara de vigilancia hasta asistentes de voz, los cuales se pueden configurar a la red de la casa y ser manipulados a distancia con una conexión a internet.

Ilustración 5: Marcas y servicios disponibles para ser usados en el hogar

Tomado de: Avast Blog *[10]*

Estos dispositivos son bastante vulnerables como se mencionó en el numeral II.CII.C de la Justificación, en el cual Avast informo ente Blog las predicciones de vulnerabilidades para este año 2019 [10]

Otra forma en la cual los ciberdelincuentes se aprovechan del usuario es a través del spam y phishing, estos cada vez más y mejores elaborados, cuyo objetivo es hacer caer a su presa sin que esta dude de su autenticidad como se puede observar en la Ilustración 6. Kaspersky informo que en este primer trimestre, el spam y phishing aumentaron en los eventos populares como el día de San Valentín (mes de febrero), la presentación de los nuevos productos Apple (llevado a cabo en el mes de marzo), adicionalmente lo atacantes usaron los tracciónales correos de bancos, confirmación de compras en línea de servicios y envíos de archivos maliciosos para alarmar y atraer a las víctimas. [22]

Ilustración 6: Página falsa de inicio de sesión de Apple ID

Tomado de: Kaspersky SecureList *[22]*

Estadísticas de Kaspersky sobre spam y phishing durante el primer trimestre del 2019 [22]

Durante el mes de mayo del presente año el Blog de Kaspersky público su primer informe del año

acerca de los ataques de spam y phishing que ocurrieron a nivel mundial durante el primer trimestre del presente año, a continuación, los resultados:

Phishing

Con respecto a este tema, la proporción de usuarios atacados aumento un 12.11%, estadística informada por Kaspersky con base a los usuarios que adquirieron sus productos. “el país con la mayor proporción de usuarios atacados por los phishers en el primer trimestre de 2019 fue Brasil: 21,66%. El trimestre anterior también estaba en el primer lugar, pero desde entonces ha ganado un 1,53%.” [22]

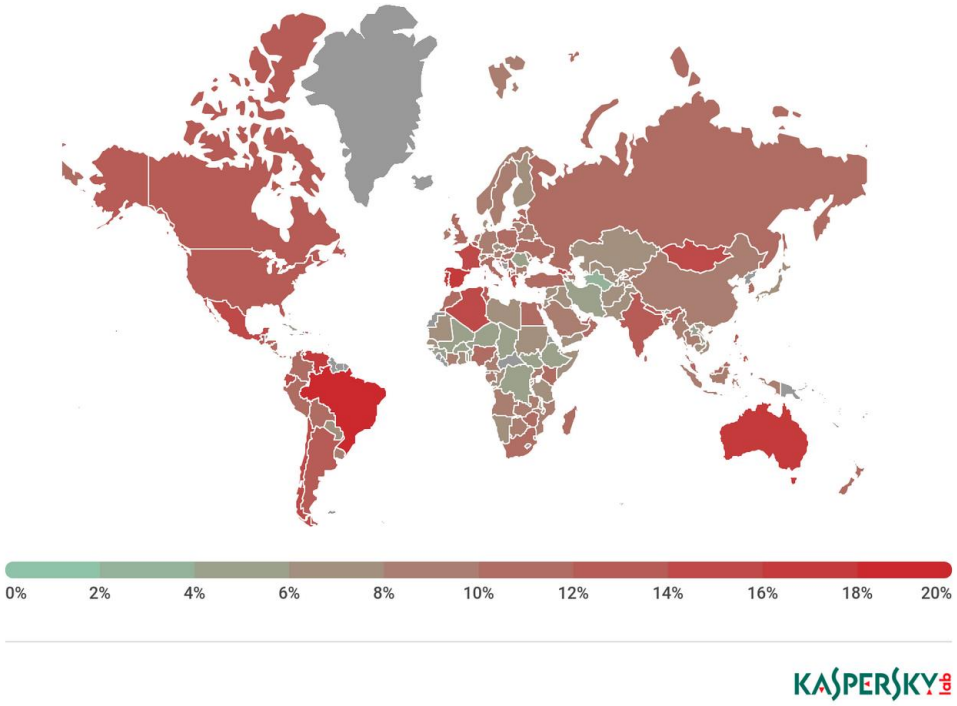


Ilustración 7: Geografía de los ataques de phishing, primer trimestre de 2019

Tomado de: Kaspersky SecureList *[22]*

Como se puede ver en la Ilustración 8, Brasil está en la cabeza del : Top 10 de los países con el mayor ataque de phishing durante el primer trimestre del 2019, seguido de Australia y España

País	%*
Brasil	21,66
Australia	17,20
España	16,96
Portugal	16,81
Venezuela	16,72
Grecia	15,86
Albania	15,11
Ecuador	14,99
Ruanda	14,89
Georgia	14,76

*Porcentaje de usuarios en cuyos equipos reaccionó el sistema Antiphishing, del total de usuarios de productos de Kaspersky Lab en el país

Ilustración 8: Top 10 de los países con el mayor ataque de phishing durante el primer trimestre del 2019

Tomado de: Kaspersky SecureList *[22]*

Spam

"El promedio del spam en el tráfico global de correo aumentó en un 0,06 % y constituyó el 55,97%, […]cifra casi idéntica (un 0,07% superior) a la del cuarto trimestre de 2018" [22] como ser puede visualizar en la Ilustración 9. Con respecto a los países fuentes de spam, "China (15,82%) y Estados Unidos (12,64%) ocuparon los primeros lugares en el ranking de fuentes de spam." Colombia se ubica en el puesto número 18 con un 1% y los países que son víctimas del envió de spam el primero es "Alemania con un índice del 11,88%. Le sigue Vietnam (6,24%). Rusia ocupa el tercer lugar, con una participación del 5,70%." [22]

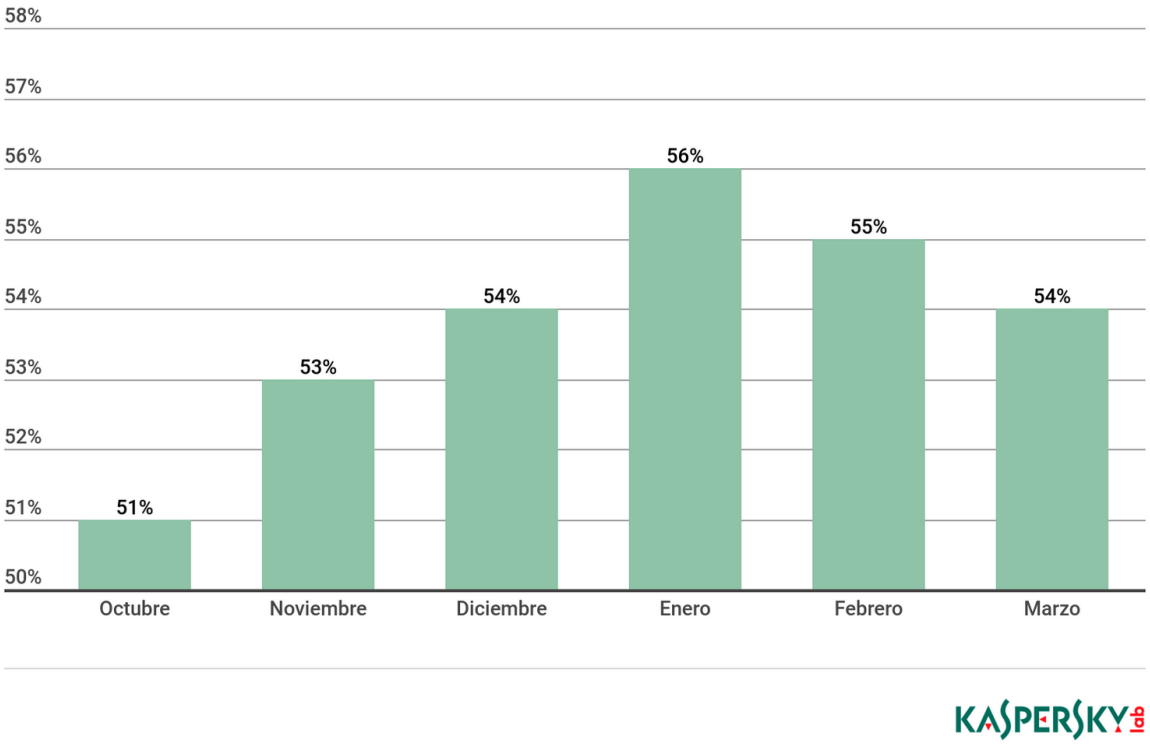


Ilustración 9: Proporción de spam en el tráfico de correo del sector ruso de Internet, cuarto trimestre de 2018, primer trimestre de 2019

Tomado de: Kaspersky SecureList *[22]*

Con este informe se concluye que "los estafadores no pierden la oportunidad de utilizar para sus propios fines los acontecimientos de gran resonancia (presentación de Apple, ataque terrorista en Nueva Zelanda […] Aparte de sus otros métodos, los atacantes siguen utilizando las redes sociales para lograr sus objetivos. Y para la "ampliar su cobertura")" [22]

Con respecto a Colombia, durante los primeros 4 meses del año en curso el Cai Virtual de la Policía Nacional público en su plataforma virtual [23] un total de 6345 delitos, los cuales fueron reportados por las entidades atacadas, el mayor afectado fue el sector ciudadano el cual reporto 5298 denuncias por delitos informáticos, la modalidad que más se usó fue de Phishing con un total de 1198 incidentes, seguido por Malware con 1019 y el delito que más denuncias se reportaron fue el de estafa (artículo 1819) con 1819 denuncias. Estas estadísticas se pueden observar en la Ilustración 10.

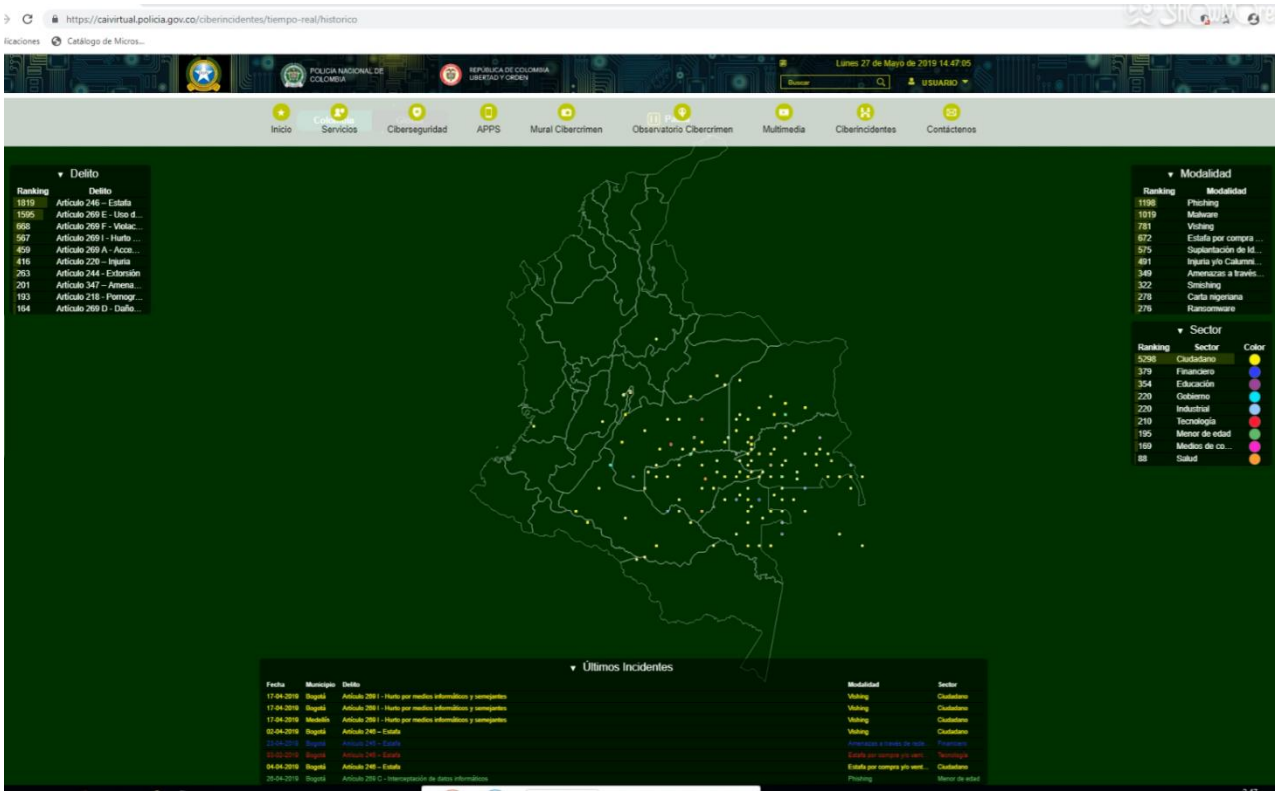


Ilustración 10: Reporte del Cai Virtual de la Policía Nacional

Tomado de: Cai Virtual de la Policía Nacional de Colombia *[23]*

V. METODOLOGÍA

A. Fases del trabajo de grado

Este trabajo estará orientado por las siguientes fases:

a) Fase 1: Diseño

En esta primera fase se realizará el diseño del ataque a la red hogareña, en la cual se usarán las siguientes herramientas:

- Vulneración de la red Wifi: se usarán los programas CommView for Wifi y Aircrack-ng los cuales nos ayudara a forzar la seguridad de la red para validar si la seguridad es óptima o fácil de romper
- Escaneo de la red: su usara el programa Wireshark, Wifi Thief Detector y SoftPerfect Network Scanner las cuales ayudaran a tener una idea del tráfico que circula a través de la red y de visualizar los equipos conectados a la red.
- Escaneo de vulnerabilidades en los equipos de la red: Nessus Essentials, el cual ayudará a identificar las vulnerabilidades que tienen los dispositivos conectados a la red, ya sean puertos abiertos, actualizaciones faltantes o problemas de configuración.

Una vez finalizada la fase diseño del ataque, éste será probado en una red propia con el fin de validar su estructura e iniciar la documentación lo cual se explicará en las siguientes fases

b) Fase 2: Desarrollo manual de buenas prácticas

Se desarrollará el manual de auto ataque para el usuario final, para esto, se llevará a cabo un auto ataque y documentación del proceso paso a paso, para ser replicado posteriormente en la mitad de la población de muestra, en esta fase, se estará trabajando a través de Word ya que a medida que se vaya implementando, se le estarán haciendo los respectivos ajustes sobre el documento con el fin de evitar ambigüedades, para esto se realizará acompañamiento directo a la población escogida,

durante la ejecución del procedimiento.

c) Fase 3: Implementación y ajustes

Con el manual ajustado después del trabajo desarrollado con el primer grupo poblacional y los resultados obtenidos al finalizar su aplicación, se procederá a probarla en la segunda muestra poblacional sin acompañamiento, con este proceso se espera total claridad y validación de las estrategias planteadas en el manual.

d) Fase 4: Resultados y difusión

Con la información obtenida de las 2 muestras poblacionales, los cuales se procederán a analizar, se sacará una estadística de las vulnerabilidades encontradas en cada red, se procederá a retroalimentares los resultados obtenidos con las herramientas (estos resultados le aparecen al usuario al ejecutar cada herramienta) y a informarles acerca de cómo remediar los problemas encontrados. Por último, se les aplicará una prueba en el cual se realizará un diagnostico final de los resultados obtenidos junto con los conocimientos adquiridos por los participantes. La difusión del manual de auto ataque estará disponible para su uso y conocimiento general, bajo previa declinación de responsabilidad del autor (Ing. Anggie Katherin Ovalle Vélez) y la Universidad Católica de Colombia.

B. Instrumentos o herramientas utilizadas

Para este proyecto se usarán las siguientes herramientas para sus diferentes etapas (planeación, ejecución y resultados)

Recursos:

- Conexión a internet de 10 Mb, para ser usado en consultas y descarga de software que se usara durante este proyecto

- 1 equipo portátil HP 1000 y 1 equipo Escritorio HP Compaq Pro-6300 SFF con las siguientes herramientas de software instaladas:
- Sistemas Operativos:
    - Windows 10 Pro: Se usará este software para las etapas relacionadas con la documentación de los procesos de planeación, ejecución y resultados del proyecto
    - Kali Linux 2019.1: se debe establecer su uso en este proyecto para la fase de ejecución debido a que cuenta con múltiples herramientas para la instrucción, para este caso de redes Wifi.
- Software:
    - Microsoft Word o software equivalente: para llevar acabo la edición de los diferentes entregables (entre ellos el presenta documento)
    - Microsoft Project o software equivalente: Para la planificación del cronograma y recursos del proyecto.
    - Wireshark: software para el escaneo de los paquetes que están viajando por la red
    - Nessus Essentials: para realizar los respectivos análisis de las vulnerabilidades de los equipos conectados a la red
    - SoftPerfect Network Scanner: Software de escaneo de red que permite descubrir equipos conectados a la red, sus carpetas compartidas y recuperar información sobre dispositivos de red a través de diferentes protocolos de red
    - Wifi Thief Detector: software que se usara para hacer el descubrimiento de equipos conectados a la red
    - Aircrack-ng: Software que se usara para realizar el ataque a la red Wifi
    - CommView for Wifi: programa para la captura de paquetes de redes Wifi

C. Población y muestra

La ejecución del proyecto será trabajada con 10 personas, las cuales están ubicados en el barrio la Gloria en la carrera 9 Este entre diagonal 45b sur al norte y la quebrada la Chiguaza al sur, localidad

de San Cristóbal, Bogotá, Colombia (Ver Ilustración 11), en cuyos hogares tienen contratado el servicio de internet junto con el servicio de Wifi, los cuales, bajo consentimiento, se les hará entrega de un manual (previamente desarrollado) la cual contendrá el paso a paso a seguir para desarrollar los ataques dentro de su red. Durante su ejecución tendrán ayuda y supervisión del líder del proyecto (Ing. Anggie Ovalle), haciendo los respectivos ajustes del documento a medida que las personas involucradas en este proyecto informen los puntos que no les son claros para su ejecución.

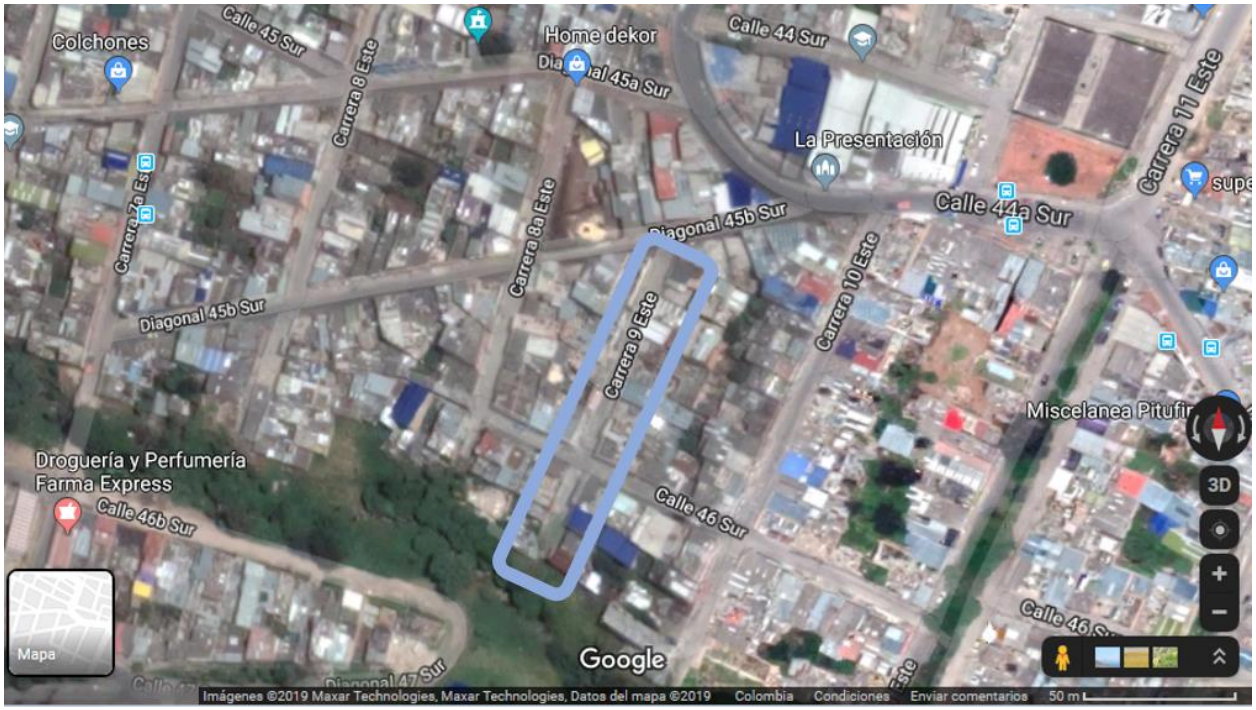


Ilustración 11 Ubicación geográfica de la muestra poblacional

Tomado de: Google Maps *[24]*

D. Alcances y limitaciones

El proyecto tendrá como alcance el desarrollo de un manual de ataques a las redes hogareñas y las respectivas recomendaciones de buenas prácticas para la configuración de red y reducción de riesgos de seguridad.

La limitación que se le presentaría este proyecto al momento de su ejecución es la negación por parte las 10 personas escogidas de hacer partícipe de este proyecto, debido a que el manual abarca la explotación (por parte del dueño de la red) del tráfico de la red en cuestión para obtener la clave de ingreso a esta, el análisis de su tráfico, el inventario de los elementos tecnológicos conectados a través de esta red y con la ayuda de Nessus descubrir las vulnerabilidades de estos equipos, de aceptar, los dueños pueden exigir la protección de su identidad y datos obtenidos en este proyecto en caso de que su buen nombre se vea en peligro, solicitando para esto el cambio de su nombre verdadero por uno falso para proteger su identidad o su restricción total de la publicación de sus resultados.

VI. PRODUCTOS A ENTREGAR

Los entregables para este proyecto se detallan a continuación:

- Acta de aceptación para la participación de este Proyecto por parte de los implicado, el cual le explica de forma concisa al implicado los alcances y objetivos del proyecto.
- Encuesta de Diagnóstico, la cual será aplicada a los participantes del proyecto, en la que se realizará un diagnóstico del conocimiento acerca de la protección de sus redes hogareñas.
- Manual de Ataque, en el que se detalla el paso a paso la instalación y uso de los programas usados por cada capítulo. Este manual está dividido en 3 partes:
    - Vulneración de la red Wifi
    - Escaneo de red
    - Escaneo de Vulnerabilidades
- Encuesta de resultados, la cual será aplicada a los participantes del proyecto en su finalización, allí se realizará un diagnóstico de los resultados obtenidos y los conocimientos adquiridos.

En el siguiente capítulo se explicará en detalle los resultados alcanzados con cada uno de estos entregables.

VII. ENTREGA DE RESULTADOS ESPERADOS E IMPACTOS

A. Encuesta de diagnostico

Se toma un grupo de 10 personas (ver la sección Población y muestra) al cual se le aplica una encuesta inicial, cuyo tema es un diagnostico acerca de sus conocimientos relacionados a seguridad informática orientado a las redes domésticas, a los dueños de estas redes (los cuales son aquellas personas que pagan el servicio de Internet), a continuación se comparten las preguntas y resultados de la encuesta:

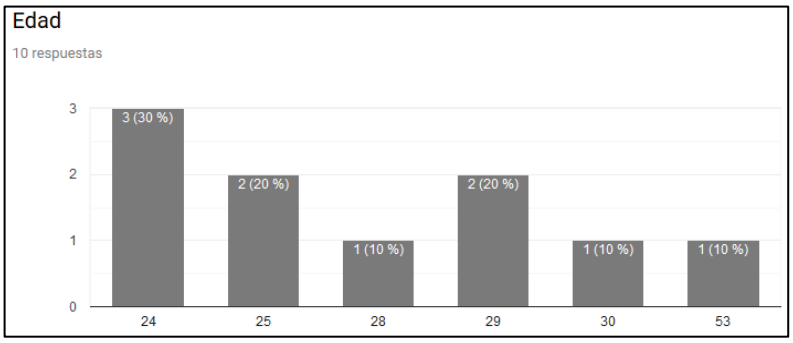


Ilustración 12 Edad de los participantes de la encuesta

Tomado de: Elaboración propia

La edad promedio de los encuestados es de 29 años, los cuales el 90% de los encuestados tienen una edad que ronda por debajo de los 30 años

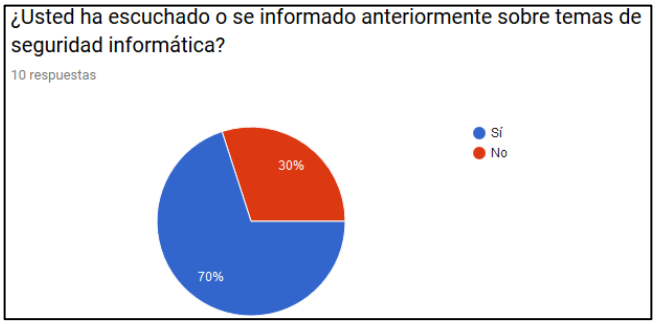


Ilustración 13 Respuestas acerca del conocimiento sobre de temas de seguridad informática

Tomado de: Elaboración propia

Dialogando un poco más a fondo con los encuestados sobre este punto, el 30% de las personas que respondieron que no se habían informado sobre temas de seguridad informática argumenta que debido a factores como (citado las palabras que dijeron) “falta de tiempo” y “desconocimiento de los términos” no habían tenido la oportunidad de investigar e informarse sobre este tipo de temas

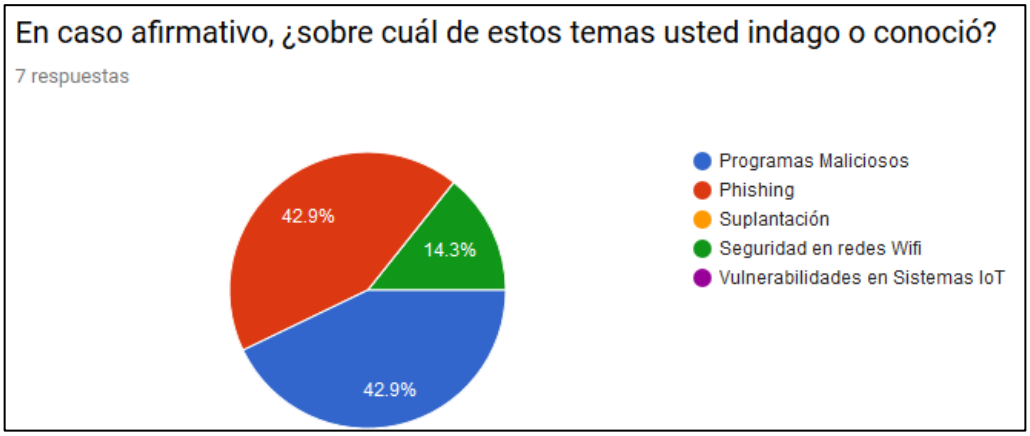


Ilustración 14 Respuestas ante temas de seguridad investigados por los encuestados

Tomado de: Elaboración propia

Los encuestados que respondieron afirmativamente a la pregunta anterior, se les pregunto acerca de que temas habían indagado, se visualiza que el mayor porcentaje se ve en los temas sobre programas maliciosos y Phishing, preguntándoles acerca de sus respuestas, los encuestados comentan que dado a las noticias y alertas que han visto en las redes sociales sobre el robo de la información y cómo funcionan, han investigado de este tipo de temas para estar informados y así tomar medidas para su protección al momento de navegar en la red.

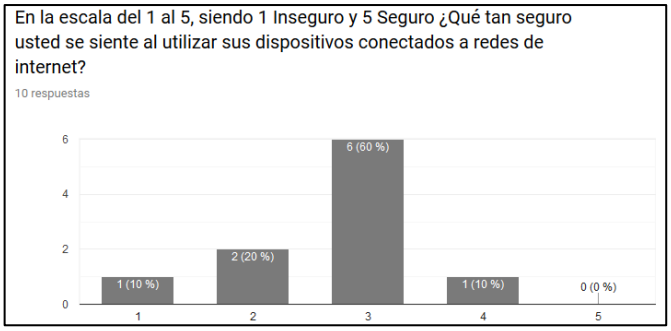


Ilustración 15 Respuestas ante la concepción de seguridad sobre la navegación de redes de internet usando sus propios dispositivos

Tomado de: Elaboración propia

La mayoría de los encuestados manifiesta que son neutros con respecto a la navegación de sus dispositivos en redes diferentes a la suya, comentan que son cautelosos en la navegación, adicional informan que usan sus redes sociales dentro de esta red, que, si requieren hacer operaciones bancarias o que involucren información sensible, prefieren usar redes conocidas.

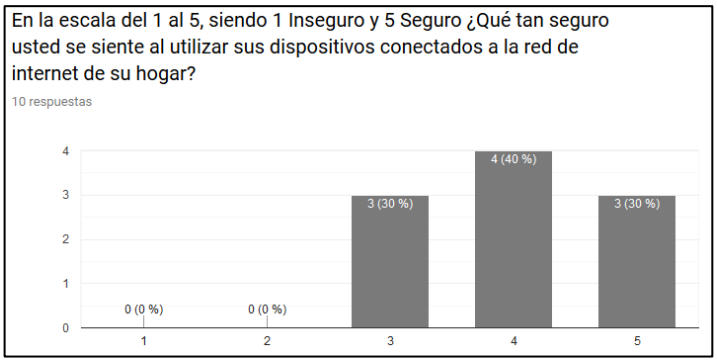


Ilustración 16 Respuestas ante la concepción de seguridad sobre la navegación dentro de su red de internet usando sus propios dispositivos

Tomado de: Elaboración propia

En el caso de la navegación en redes propias, los usuarios se sienten más seguros, ya que, según ellos, al navegar en una red que es conocida (su propia red de internet), tienen la seguridad de los dispositivos que se encuentran conectados de la red son conocidos y que no hay desconocidos navegando dentro de esa red, adicional, comentan que la información que circula por su red no será afectada.

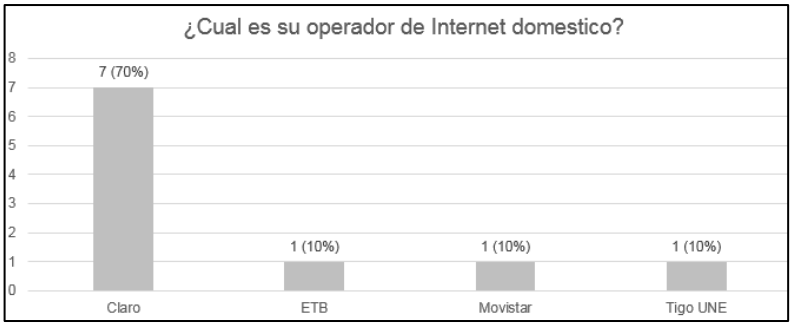


Ilustración 17 Resultados sobre el prestadior de servicios de internet de los encuestados

Tomado de: Elaboración propia

Se puede visualizar que el mayor operador de servicios de internet es el servicio de Claro, cabe informar que los encuestados defienden su proveedor sobre la competencia, ya que este les ha prestado un buen servicio, pero todos concuerdan que el soporte y los procesos administrativos ante su proveedor es bastante complicado.

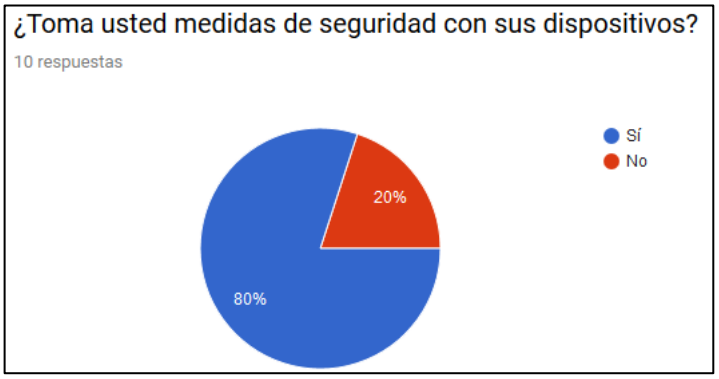


Ilustración 18 Resultados acerca de si los encuestados toman medidas de seguridad en sus dispositivos

Tomado de: Elaboración propia

La minoría de los resultados acerca de esta pregunta, comentan que no ven necesario tomar medidas de seguridad ya que piensan que los dispositivos en donde se encuentran almacenada su información e interactúan no lo requieren y su información se encuentra bien respaldada.

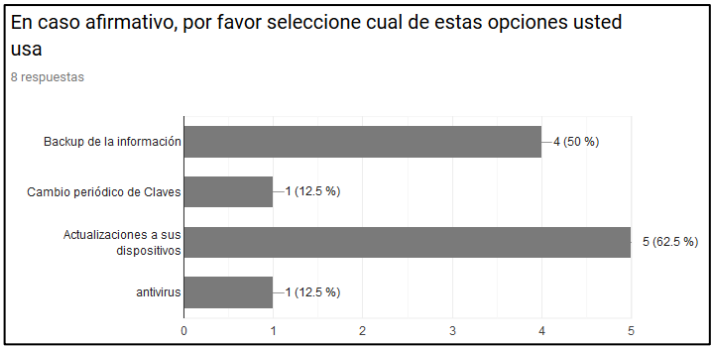


Ilustración 19 Resultados acerca de las opciones que usan los encuestados para proteger sus dispositivos

Tomado de: Elaboración propia

Los encuestados que respondieron de forma positiva la penúltima pregunta asocian como medida de seguridad la actualización de los dispositivos que usan habitualmente (con un porcentaje de 62.5%), seguido del Backup de su información (50%), en este punto, se les pregunto la forma que usan para respaldar la información y comentan que usan sus cuentas de correo (Hotmail y Gmail), las cuales ofrecen el plus de espacio en la nube para guardar información, así que ellos aprovechando ese beneficio, suben la información más importante a estos servicios.

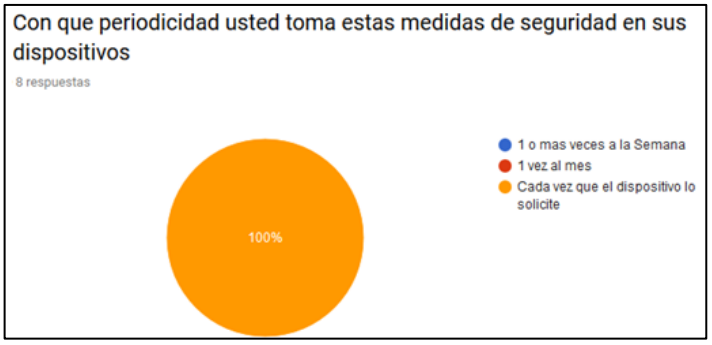


Ilustración 20 Resultados acerca de la periodicidad de las medidas de seguridad que toman los encuestados sobre sus dispositivos

Tomado de: Elaboración propia

Con respecto a la pregunta anterior, todos toman este tipo de medida cada vez que el dispositivo les informa, ya sea Backup, cambio de claves o actualizaciones del dispositivo, los

encuestados no tienen la costumbre de hacer este tipo de actividades de forma autónoma.

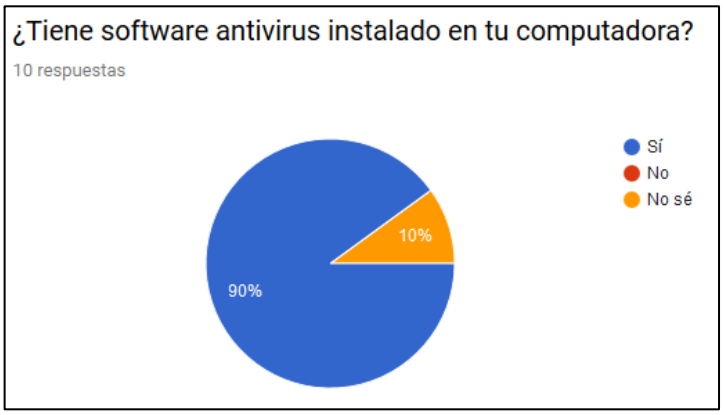


Ilustración 21 Resultados sobre el uso de un antivirus en las computadoras de los encuestados

Tomado de: Elaboración propia

El 90% de las personas encuestadas afirman que usan un software de antivirus en sus equipos ya que, al momento de configurar sus equipos, fueron asesorados en el proceso por un conocido, que les comentaba que este tipo de software les ayudaba a evitar problemas de virus en sus equipos.

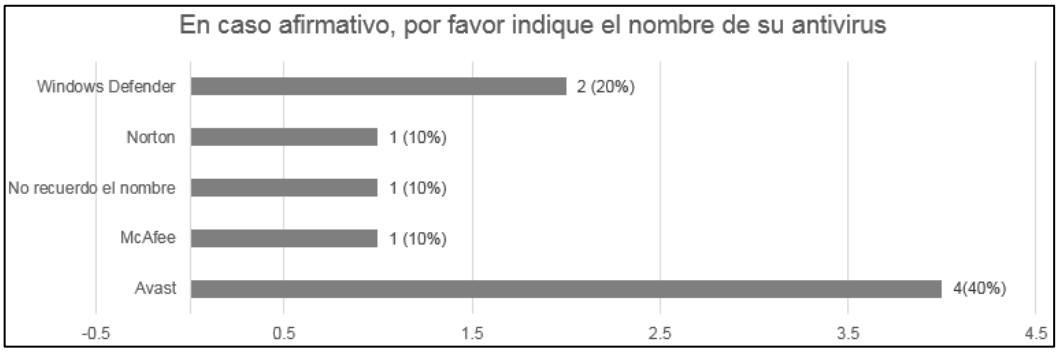


Ilustración 22 Resultados sobre la marca de antivirus que usan los encuestados en sus computadores

Tomado de: Elaboración propia

Respecto a las respuestas de esta pregunta, el antivirus usado, comentan los encuestados, lo recomendó la persona que los asesoro, al preguntarles sobre si conocían otra marca de antivirus

ellos respondieron que no, adicional, al preguntarles sobre cómo les estaba yendo con su antivirus actual, comentaron que no han tenido problemas con este.

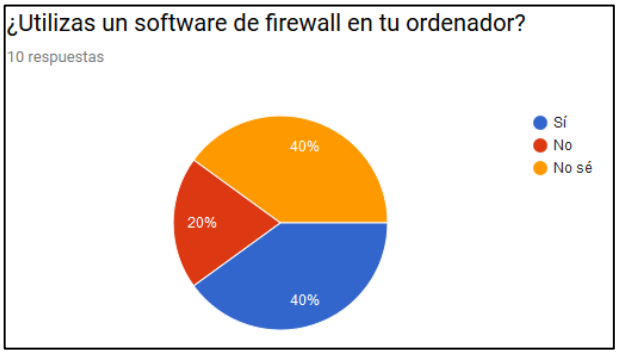


Ilustración 23 Resultados acerca del uso de software Firewall

Tomado de: Elaboración propia

Ante esta pregunta los encuestados que contestaron de forma afirmativa, informaron que el firewall que usan es el que viene con su sistema operativo de Windows (firewall de Windows), el cual saben de su existencia debido a que han tenido que interactuar con él en diferentes etapas de su vida educativa universitaria y también han investigado por su cuenta su funcionamiento. Las personas que respondieron negativamente y que no sabían, no tienen en claro el concepto ni para sirve.

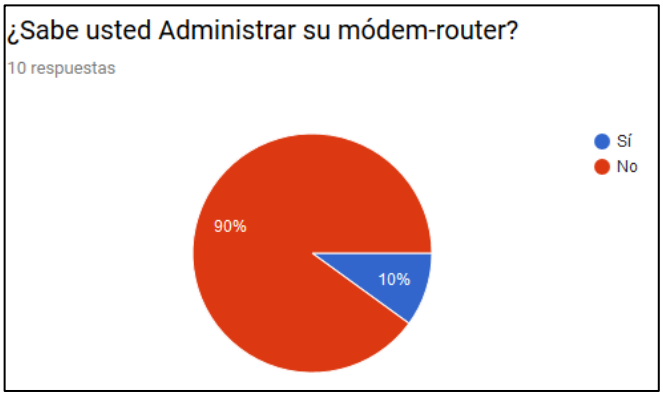


Ilustración 24 Resultados acerca de la administración del Modem-Router de los encuestados

Tomado de: Elaboración propia

Con respecto a esta pregunta, solo una persona informa que sabe administrar su dispositivo, se le pregunto qué tipo de configuraciones hace y respondió que administra desde allí su red Wifi y permite la navegabilidad de sus dispositivos por medio del registro de sus MAC, ya que en caso de tener un dispositivo indeseado, este no podrá navegar por su red, la persona comenta que esta opción la trae su modem-router y que le fue enseñada por el tecnico del operador de internet que le instalo el servicio. El resto de los participantes, no han tenido la necesidad de interactuar con la administración de su dispositivo, ya sea porque no tienen los conocimientos acerca de cómo hacerlo o su proveedor no les entrego credenciales de administración, para este punto, varios respondieron que, en caso de requerir algún camio, ellos se contactan con su proveedor de servicio, el cual les ayuda con los cambios que soliciten (esto van ligados al cambio de clave y/o nombre de su de Wifi)

B. Aplicación de los manuales y análisis de sus resultados

Al momento de comenzar el desarrollo y aplicación de los manuales, se tomaron 2 grupos, el primero fue usado para ajustar los manuales, los cuales fueron elaborados previamente, para ser entregados al grupo No. 2, a continuación, se mostrará los resultados de cada uno de los manuales implementados a los participantes, los cuales después de obtenidos los resultados, estos se les fueron explicados de forma clara y concisa a cada uno de los participantes.

a) Vulneración de la red Wifi

Con el primer manual, los integrantes de la encuesta probaron la eficacia de su clave de red wifi, la cual, consiste hacer la captura de handshake (son los paquetes que se intercambian entre el punto de acceso de la red Wifi y un cliente para su conexión), para esto con la ayuda de commview for wifi, la cual usa la tarjeta de Wifi, para la detección de la red deseada, envió de paquetes a los dispositivos conectados a esta red para generar su des autenticación y así generar el procese de autenticación entre estos dispositivos, creando el handshake deseado. Ya teniéndolo, se procede con su descifrado, para esto se usa Aircrack-n junto con un archivo de diccionario, se les informa a los participantes que pueden bajar este tipo de archivos en diferentes foros de internet o pueden crear su propio diccionario, todos optaron por buscar y bajar el archivo, a continuación,

los resultados del ataque:

Tabla 1-1 Resultados de la obtencion de la clave Wifi por medio del handshake de la red y ataque de diccionario

Red	Propietario	Resultado	Observaciones
FAMILIA HERNANDEZ	Andres Hernandez	Clave no Descubierta	N. A
NOCTURNO	Juan Sebastian Torres	Clave no Descubierta	N. A
ARRIS-7672	Johanna Leon	Clave no Descubierta	N. A
DIAZ	Paola Suarez	Clave Descubierta	La clave de la red es una combinación de números sencilla de 8 caracteres - número de teléfono de la casa-
ARRIS	Paola Vázquez	Clave no Descubierta	Por incompatibilidad con la tarjeta de red de su equipo, se procede a apoyar al participante con este punto.
REN	Nora Mendieta	Clave Descubierta	La clave de la red es una combinación de números sencilla de 10 caracteres - número de cedula de su hija -
LUZMERY	Angie Hurtado	Clave Descubierta	La clave de la red es una combinación de números sencilla de 8 caracteres - Numero de cedula de su madre -
DANNA2	Nurit Zambrano	Clave Descubierta	La clave de la red es su mismo SSID, pero finalizado en 123, obtenida en un segundo ataque de diccionario
FAMILIA MOMO	Andres Montaño	Clave no Descubierta	N. A
ASGARD	Viviana Sarmiento	Clave no Descubierta	N. A

De las 10 redes atacadas por sus dueños solo 3 obtuvieron resultados favorables ya que en los diccionarios que descargaron, contenían en su interior la clave, los usuarios enviaron sus archivos .cap para su análisis y ejecución de un segundo ataque de diccionario, el diccionario usado para este puto contenía palabras en el idioma español, combinaciones numéricas y palabras relacionadas con el participante y su red (información obtenida por medio de charla al momento

de la aplicación del cuestionario de diagnóstico), mezcladas con caracteres numéricos, en este análisis solo se descubrió una clave más, para un total de 4 claves obtenidas sobre 10, con los usuarios a los que no les descubrió la clave se les pregunto acerca del contenido de esta (sin que ellos la revelen) las características que tienen en común es que usan un carácter especial (la mayoría *) y que combinan su clave con al menos una mayúscula y varios números. Como parte de la plática con los participantes, se les pregunto acerca del origen de sus claves las respuestas se dividieron entre

- Clave dada por el proveedor de internet al momento de la instalación del servicio
- Clave entregada al proveedor del servicio para su configuración (en este grupo se encuentran las 3 redes a las que se les descubrió la clave)
- Clave que se cambia cada cierto tiempo (esta respuesta fue dada por el único encuestado que administra su Router)

Como parte de retroalimentación de esta parte con las redes comprometidas (ver Tabla 1-1), se les hablo acerca del cambio de clave, el cual en caso de no saber cómo llevarlo a cabo, pueden apoyarse con su proveedor de servicios de internet (el cual esta obligados a prestarles la ayuda necesaria), respecto a la elección de la clave se les recomienda usar caracteres alfanuméricos y especiales, en lo posible evitar el uso de información personal al momento de generar la clave (fechas de cumpleaños, números de identificación, número de teléfono, nombres de algún integrante de la familia, etc.)

Adicional, en la red de ARRIS, su dueño tuvo problemas con el desarrollo de este primer manual, debido a que su equipo portátil tenía problemas de compatibilidad con la tarjeta de red, motivo por el cual con este usuario bajo su autorización se le fue aplicado este manual usando un equipo externo que ya tenía la herramienta funcional.

b) Escaneo de red

Con el segundo manual, su objetivo era que los participantes visualizaran los equipos que

se encontraban conectados en la red y la visualización del tráfico durante la ejecución de la guía, para esto se usó SoftPerfect Network Scanner el cual escanea y hace el inventario los dispositivos que se encuentran en red, adicional, informa si los equipos tienen puertos abiertos y carpetas compartidas (este último detalle en equipos de cómputo de mesa y portátiles), también se lleva acabo el uso de Wifi Thief Detector, una aplicación para dispositivos con sistema operativo Android, el cual informa la cantidad de dispositivos conectados en ese momento en la red, su IP, MAC, nombre y sistema operativo.

Tabla 1-2 Redes con novedades en su interior

Red	Propietario	Resultado
FAMILIA HERNANDEZ	Andres Hernandez	En esta red se encuentra un equipo de cómputo con la carpeta de User visible
ARRIS	Paola Vázquez	En esta red se encuentra un dispositivo que el usuario no conoce (dispositivo marca Sony) y un computador con la impresora compartida
REN	Nora Mendieta	Un computador de escritorio con la carpeta de User compartida.
DIAZ	Paola Suarez	En esta red se encuentra un equipo de cómputo con la carpeta de User y una carpeta llamada “Otros” visible
DANNA2	Nurit Zambrano	En esta red se encuentran 2 dispositivos desconocidos (celular marca Xiaomi y un computador portátil bajo el nombre de HP-casa) que no son conocidos por el usuario

Al dialogar con los responsables de cada red, los participantes que tienen hosts desconocidos informan que pudieron detectarlos fácilmente gracias a Wifi Thief Detector, uno de ellos (Red DANNA2) informa que en pasadas semanas la vecina de la casa del lado le comento que si le podía compartir un poco de su red de internet, debido a que su hijo tenía una serie de tareas que requerían el servicio y su servicio de internet no estaba funcional, por este motivo la dueña de la red accedió al favor, comenta que desde esa época ha notado el internet lento en especial los fines de semana, pero no entendía el por qué.

Con lo que respecta a la red de ARRIS, el usuario informa el dispositivo de marca Sony no es suyo, ya que a la red solo tiene conectado su computador portátil sus 2 celulares (Apple y Huawei) y un decodificador que les fue instalado por el proveedor del servicio, motivo por el cual

desconoce la procedencia de este dispositivo. Respecto a su computador se le informo que tiene compartida una impresora.

Las redes REN y FAMILIA HERNANDEZ y DIAZ se encontró en cada una cada una carpeta compartida la cual es User (esta carpeta contiene la información de cada usuario que tenga creada la máquina, desde documentación hasta configuración y archivos de programas usados), el caso de la red DIAZ, el software detecto una carpeta adicional compartida llamada Otros.

Recomendaciones a los dueños de Redes Wifi con novedades

Ante los hallazgos de intrusos, se les recomendó a los afectados el cambio de la clave de acceso a la red, que para esto, podían apoyarse con el centro de soporte tecnico de su proveedor como se informó en la sección *Vulneración de la red Wifi*, siguiendo los alineamientos recomendados para la creación de la clave de acceso, en el caso de la red DANNA2 se les recomienda que en caso de compartir la clave, después del tiempo pactado de su uso, proceda con el cambio, para evitar problemas con el funcionamiento del servicio.

Con respecto a las carpetas, se les informo de forma partica el funcionamiento de estas carpetas, que en caso de no ser usadas quitar el permiso de compartir y de usarlo (o quererlo usar en el futuro) como asignar permisos y evitar daños en la información almacenada allí por personas no deseadas

Para el tema de visualización de tráfico, los participantes usaron el software WireShark, el cual los participantes dejaron en ejecución por varios minutos para la visualización la información que circulaba por la red desde los diferentes hosts conectados a esta.

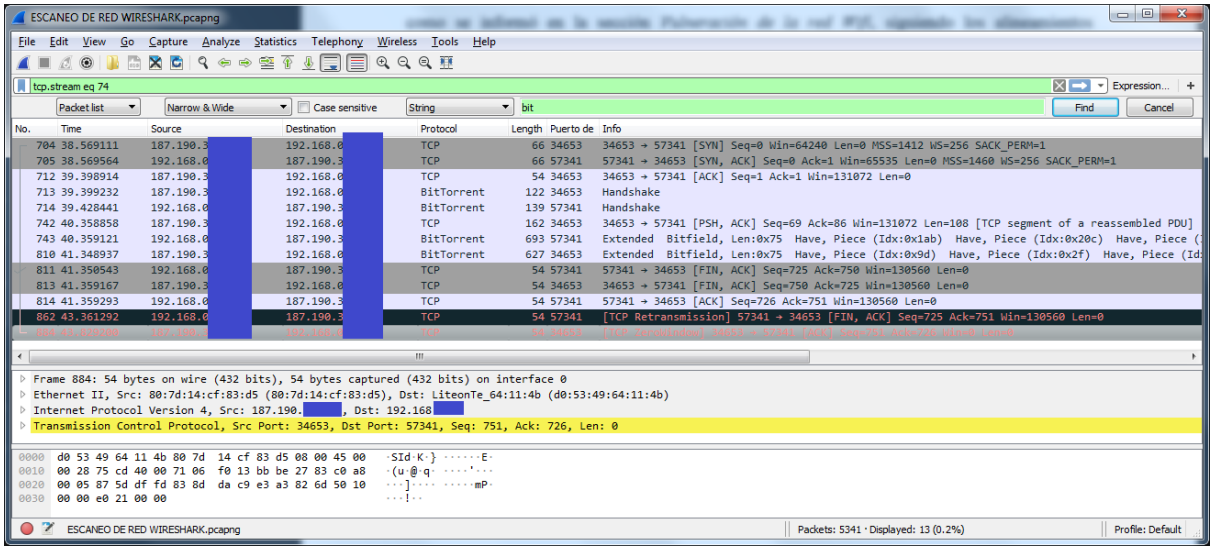


Ilustración 25 Resultado inusual en la red DANNA2

Tomado de: Elaboración propia

A nivel general, no había nada irregular a excepción de la red DANNA2 que tenía activa conexiones de BitTorrent (intercambio de archivo peer to peer), la cual se visualizó activa en varios fragmentos de la conexión (ver Ilustración 25), al compartir esta información con el participante, informa que el día en que realizo el escaneo de su red, solo tenía conectado su portátil y celular, que durante ese día noto la red lenta (esta información fue levantada por ella un domingo) ya que al reproducir música por la plataforma de YouTube esta se colgaba en ocasiones. El usuario informa que el motivo de la falla de internet se deba sea a que el hijo de su vecina, a raíz del favor realizado, este tomando ventaja sobre la ayuda que es su momento se le brindo.

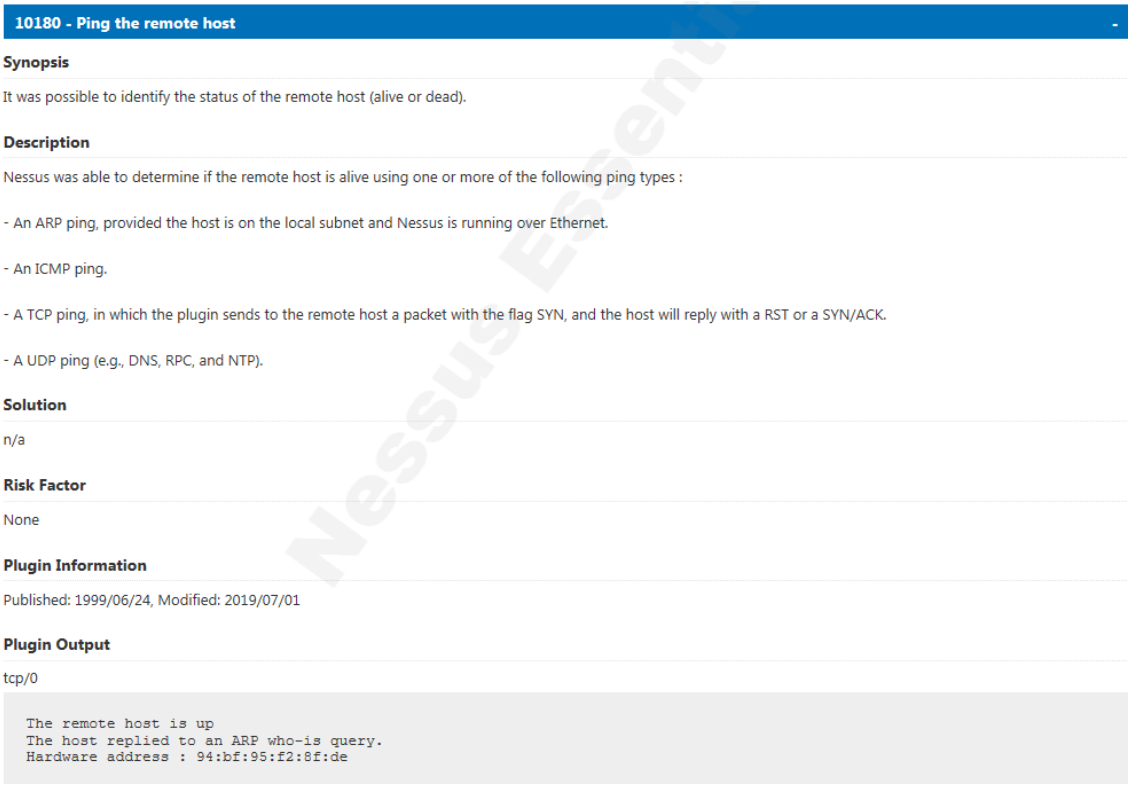
c) Escaneo de Vulnerabilidades

El objetivo del ultimo manual es de que los usuarios estuviesen informados acerca de las vulnerabilidades que se encuentran en su red. Para esto ellos usaron Nessus Essentials, el cual permite escanear la red para buscar fallos en los equipos conectados a estas (actualizaciones, puertos abiertos, configuraciones erróneas, etc.).

Respecto a los puertos abiertos:

En este apartado se les informo a los participantes que los resultados obtenidos no son alarmantes ya que la única novedad que presentan los equipos conectados, en el momento en que tomaron la muestra, es que estos dispositivos responden a la utilidad de diagnóstico llamada ping, la cual determinar si una dirección IP específica o host es accesible desde la red, como se puede ver en la Ilustración 26

Se informo que, con el uso del Firewall en sus dispositivos de computo, pueden evitar riesgo a sus equipos, como por ejemplo puertos abiertos no deseados o por no conocimiento su desactivación, este último muy grave en los equipos ya que deja sin una protección lo que permite que el equipo malware podrían encontrarse keyloggers que leen las pulsaciones que se hacen en el teclado del equipo o herramientas de acceso remoto las cuales pueden controlar un ordenador sin tener acceso físico a él.



10180 - Ping the remote host -

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/06/24, Modified: 2019/07/01

Plugin Output

tcp/0

```
The remote host is up
The host replied to an ARP who-is query.
Hardware address : 94:bf:95:f2:8f:de
```


Ilustración 26 información acerca del ping dada por Nessus en la red FAMILIA MOMO

Tomado de: Elaboración propia

Respecto a las vulnerabilidades encontradas:

Las vulnerabilidades encontradas en los diferentes equipos de cada red se clasifican en los siguientes grupos (clasificación realizada por Nessus):

- Critico
- Alto
- Medio
- Bajo
- Informativo

Allí la herramienta informa cantidad de alertas encontradas en cada host como se puede ver la siguiente imagen:

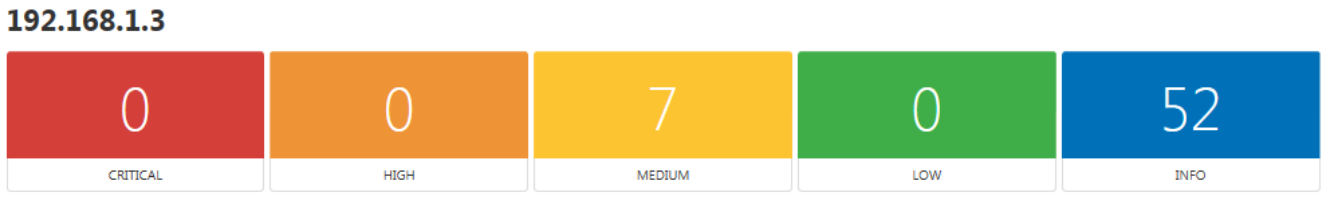


Ilustración 27 clasificación de alertas de Nessus por cada equipo examinado

Tomado de: Elaboración propia

El dispositivo con más riesgo en promedio en cada red es el router-modem (6 de las 10 muestras mostraron alarmas), la mayoría de las alertas son debido a que la versión de firmware que manejan estos dispositivos es antigua, motivo por el software les detecto varias vulnerabilidades que pueden afectar la seguridad y su funcionamiento, los problemas graves que se identificaron fueron:

- Desactualización en el servicio SSH
- Protocolo SSL 2 y 3 activo

- Versión antigua de libupnp

Para este punto se les recomienda a los afectados que se contacten con su proveedor de internet, sección de soporte, para que agenden una cita de actualización del firmware de sus dispositivos y así remediar los problemas que se encontraron en el análisis. Adicional terminada esta labor, se les recomendó pasar nuevamente el escaneo para validar que estos errores se hubiesen corregido con la actualización.

A nivel general, el software informo acerca de datos de carácter informativo e información que el router-modem pueden informar a las personas que se conectan a la red, como, por ejemplo:

- Tipo de dispositivo
- Detección de la información de la tarjeta de red
- Detección de la MAC del dispositivo
- Tipo, versión e información del servicio HTTP
- Identificación del sistema operativo y versión de este
- Tipo, versión e información del servicio SSH
- Versiones soportadas SSL / TLS e información del certificado
- Servicio de Telnet activo

Respecto a los equipos de cómputo detectados, a nivel crítico 1 computador de la red REN se encuentra con el firewall desactivado (se le informo al usuario sobre esta novedad y sobre como remediarlo) y varios con la vulnerabilidad de Eternal Blue (4 equipos afectados, entre ellos el equipo con el firewall desactivado) dialogando con los usuarios sobre este detalle, ellos informan que no estaban seguros si corrían las actualizaciones pertinentes para remediar este error (y otros más que las actualizaciones pueden remediar) ya que el sistema operativo no les informaba nada respecto a las actualizaciones. Se les informa los pasos a seguir para validar si las actualizaciones se están o no corriendo de manera satisfactoria, en caso de que no esté sucediendo y las comiencen a instalar, el equipo comenzara a disminuir su rendimiento y al finalizar pedirá el reinicio del equipo, este proceso tomara unas cuantas horas dependiendo de la cantidad de actualizaciones

pendientes que tenga que instalar, la velocidad del internet para la descarga de estas actualizaciones y el procesamiento de la maquina (para su fase final de instalación)

A nivel general, todos tenían el siguiente riesgo a nivel medio:

- Protocolo SMB activo

Respecto a los tópicos informativos, los dispositivos PC que salieron en los reportes de Nessus de los participantes arrojaron:

- Resolución del equipo por nombre
- Servicio de detención SMB
- Detección de la versión del sistema operativo
- Información remota del dispositivo
- Detección de la información de la tarjeta de red
- Detección de la MAC del dispositivo

El último grupo de dispositivos es el de los dispositivos móviles (lastimosamente en la muestra no se encontraron otros tipos de dispositivos conectados a la red, como por ejemplo consolas de video juegos o televisores inteligentes) Nessus mostro temas informativos (muy similares a los PC´s y router-modem), los cuales se pueden mencionar:

- Detección de la información de la tarjeta de red
- Detección de la MAC del dispositivo
- Resolución del equipo por nombre
- Identificación del sistema operativo

Al momento de dialogar con respecto a los resultados obtenidos con cada usuario, se les explico acerca de la estructura de los resultados obtenidos en su informe, adicional, para cada

vulnerabilidad encontrada por el software, este brinda página para obtener más información y un apartado de soluciones que pueden aplicar para solventar sus problemas (estos en su mayoría se solventan con actualizaciones a los dispositivos comprometidos).

C. Encuesta final

Como parte final del proyecto, se les aplico una encuesta sobre los conocimientos adquiridos durante la aplicación del manual, solicitándoles una pequeña reflexión acerca de esta actividad, a continuación, los resultados:

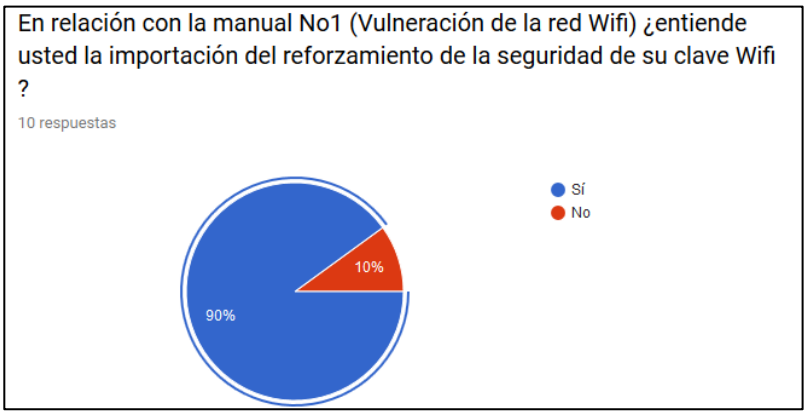


Ilustración 28 Resultados sobre la importancia del reforzamiento de la seguridad de la clave Wifi del participante

Tomado de: Elaboración propia

De las 10 personas que realizaron el manual 1 por motivos de incompatibilidad de su tarjeta de red con el software CommView for Wifi no pudo poner en práctica el manual, pero se le apoyo en este tema, adicional, al dejar un punto de argumentación de respuesta, los participantes pudieron expresar sus puntos de vista a partir de la respuesta seleccionada, entre las respuestas dadas se citan: “no conocía que existieran tantas herramientas para la detección de vulnerabilidades y descifrado de contraseñas, y que las mismas estuvieran tan a la mano. Si bien su finalidad no es maliciosa, es posible que las personas se aprovechen de esta tecnología para obtener información sobre la red de otras personas.” respuesta dada por Andres Montaño “(…) me permite saber que tan vulnerable puede llegar a ser la clave de seguridad de mi red y así permitirme poder mejorarla evitar algún tipo de ataques” respuesta dada por Andres Hernandez o “Si por que en mi caso no sabía que la clave de mi red era tan débil que esta pudo ser descubierta, lo que me obligo a su

cambio” respuesta de Nohora Mendieta (estas respuestas se pueden consultar en el anexo)

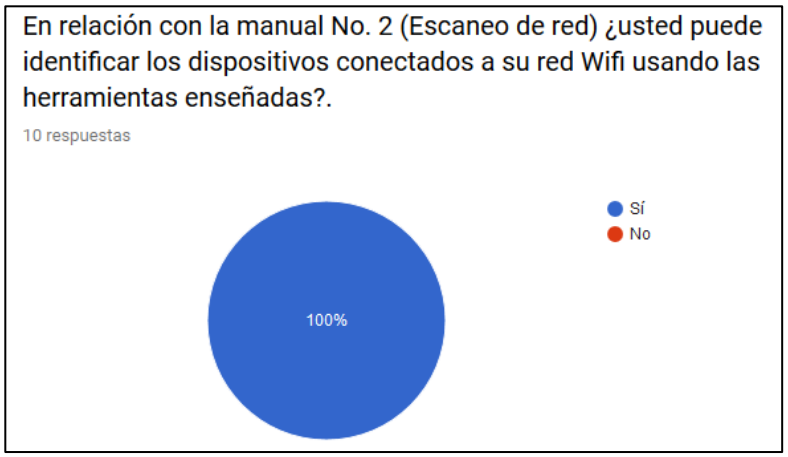


Ilustración 29 Respuesta ante la pregunta sobre la identificación de dispositivos conectados a la red

Tomado de: Elaboración propia

Los participantes pudieron identificar de forma fácil los dispositivos conectados a la red y como se dialogaba con varios de ellos, en caso de encontrar dispositivos desconocidos se recomienda el cambio de clave de acceso a la red y en caso de compartirla ser discreto en su difusión.

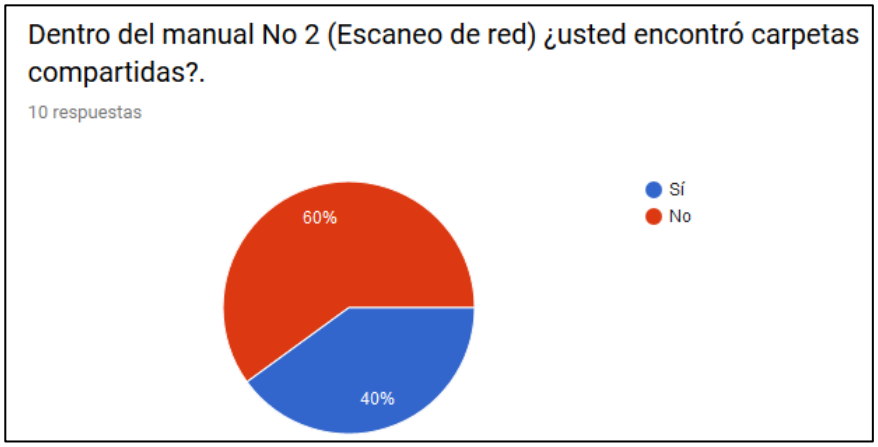


Ilustración 30 Respuestas ante el descubrimiento de carpetas compartidas dentro de la red del participante

Tomado de: Elaboración propia

En esta pregunta, solo se quería validar si lo usuarios prestaron atención a los resultados que le arrojo el software SoftPerfect Network Scanner, el cual les arrojaba los recursos compartidos que tenían los dispositivos conectados a su red al momento de la ejecución, esta

pregunta venia con otra de forma abierta en la cual los participantes escribían si sabían de la existencia de estas carpetas a lo que todos los que respondieron afirmativamente esta pregunta informaron que no sabían la existencia de las carpetas

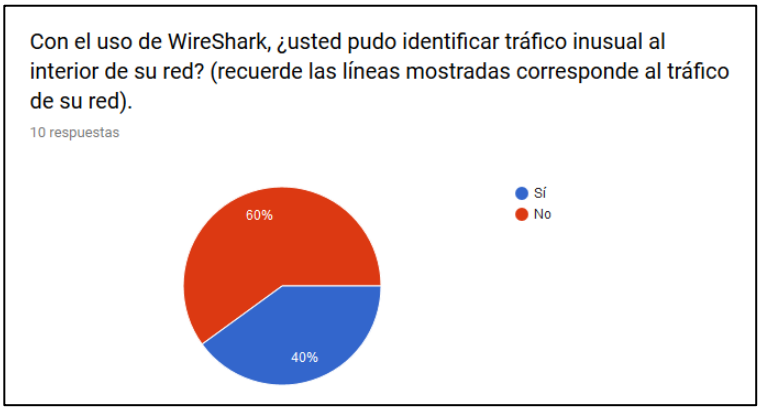


Ilustración 31 Respuestas ante la identificación del tráfico con el software WireShark

Tomado de: Elaboración propia

Como en el manual explicaba la forma de funcionamiento de este software (a nivel básico, sin llegar a tecnicismos que puedan confundir al usuario), cada participante tomaba la iniciativa de explorar lo que pasaba por su red, varios de ellos se alarmaron por paquetes que no estaban seguros de donde provenían, para este caso, cada usuario informaba de las tazas que no sabían de donde provenían, al cual se les explicaba su procedencia y ellos determinaban si era sospechoso o no según los programas instalados o páginas web que visitaban.

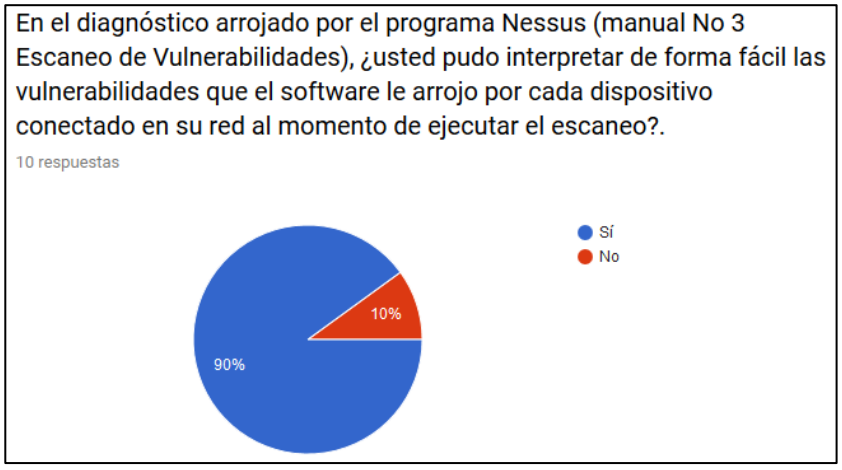


Ilustración 32 Respuestas ante la identificación de vulnerabilidades usando el software Nessus

Tomado de: Elaboración propia

En este apartado, la mayoría de los participantes entendió la estructura de informa que arroja Nessus al momento de presentar los resultados, lastimosamente un participante informa que no entendió muy bien el resultado arrojado ya que era demasiado tecnico para su comprensión y al momento de traducirlo en un servicio de traductor no entendía bien la idea de la información que le arrojaba el sistema, se puede decir que para este punto se tuvo una efectividad del 90%

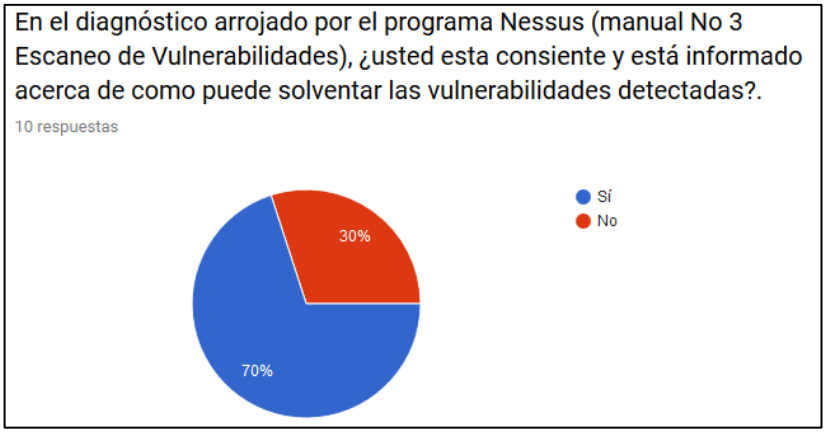


Ilustración 33 Respuestas ante la información que cuenta el participante de la red para solventar los problemas detectados en la red

Tomado de: Elaboración propia

Como parte final, el cómo pueden llegar ellos mismos a solventar estos problemas, las personas que respondieron que no, al momento de dialogar con ellas informan que algunos casos ellos deben depender de un tercero para que les ayude con su situación (como por ejemplo actualización del Firmware de su router-modem), los cual los deja con la sensación de que no tiene el control total de los dispositivos que están bajo su red y que en caso de una mala configuración ellos deben recurrir a un tercero para su ayuda y los otros al no manejar administrativamente de forma correcta piensan que pueden dañar alguna configuración ya realizada en sus equipo, motivo por el cual pueden agrandar el problema, para esto se les aconsejo buscar ayuda de una persona de confianza que los pueda asesorar y explicar los temas que no entiendan para que ellos puedan aprender y aplicar en casos similares en el futuro.

Por último, se incluyeron 2 preguntas de respuesta abierta:

- ¿Es usted consiente que la no actualización de sus dispositivos puede acarrear daños de su información?

Las respuestas fueron positivas antes este interrogante llegando desde respuestas simples ("Si" o "ahora lo soy." Esta última refiriéndose a que ya conoce los riesgos de la no ejecución de las actualizaciones), hasta de las más elaboradas, dando pequeñas reflexiones sobre el tema, como por ejemplo "si, porque de lo contrario aparte de que no voy a tener las últimas versiones de los programas al día, estos pueden afectar la seguridad de mi información" de Viviana Sarmiento, "con el desarrollo del manual si ya que no sabía para que eran las actualizaciones y que estas podían proteger mi dispositivo" respuesta dada por Nohora Mendieta o "Si por supuesto, ya que si no mantenemos nuestros dispositivos actualizados pueden presentar fallas en los sistemas operativos apps y demás funcionalidades." de Andres Hernandez.

- Que reflexión le dejo el desarrollo de los manuales

En esta parte los participantes tuvieron un espacio para expresar sus opiniones frente al desarrollo y experiencias que tuvieron durante a la ejecución del manual, es gratificante que las respuestas que dieron les dejaron experiencias y conocimiento que pueden seguir aplicando y compartiendo con personas conocidas, a continuación, se adjuntan las respuestas dadas por cada usuario en este punto:

Tabla 1-3 Respuestas a dadas por los participantes a la pregunta "Que reflexión le dejo el desarrollo de los manuales"

Participante	Respuesta
Sebastián Torres	Crear conciencia en las vulnerabilidades de la red y del equipo en el hogar, y como trabajar en alternativas que minimicen estas vulnerabilidades, con cambio constante de contraseñas, complejidad de estas y actualización de los sistemas de seguridad que proporciona el sistema operativo
Johanna León	Las redes de Wifi de los hogares son muy fáciles de vulnerar.

Viviana Sarmiento	Gracias a un manual, puedo revisar en cualquier momento la seguridad dentro de mi red o la red de un familiar y en caso de tener fallos puedo arreglarlos y no esperar a que ataquen
Nohora Mendieta	Que en mi red pueden entrar sin problemas si no tengo la protección necesaria y más si no trato los errores que tienen los equipos.
Andres Orosman Montaño Moreno	Vivimos en una época que cada vez más impulsa el uso de datos informáticos para remplazar lo analógico, desde la interacción social y las comunicaciones, hasta las transacciones bancarias a su vez esta revolución tecnológica alienta a los piratas informáticos para poder obtener beneficios maliciosos con la información transada en la red. es importante empezar a blindar la información de estos posibles ataques y este tipo de ejercicios ayuda a que uno tome conciencia de la importancia de la seguridad informática y a que uno tome algunos hábitos en este tema.
Angie Paola Hurtado Acosta	Primero aprendí a identificar los dispositivos conectados a la red Wifi y así mismo a identificar carpetas compartidas lo cual es muy importante para proteger la información. Adicionalmente estos manuales enseñan tanto a detectar como a solventar las vulnerabilidades de red, lo cual es muy importante para generar transacciones y compartir información con mayor seguridad.
Andrés Hernández	Debo estar más atento a las vulnerabilidades que puede presentar mi red, así como tener el conocimiento de los equipos que están conectados a mi red y si son de confianza para evitar futuros ataques a mi red.
Paola Suarez	Que se deben hacer actualizaciones para mantener la información segura, así como generar seguridad para red con su periódica actualización y vigilancia
Nurit Zambrano	Con la guía pude detectar un intruso en mi red (al cual le había dado acceso temporal y que continúo conectándose) lo que hacía que mi internet fuese lento. Realizando el cambio de clave con la ayuda del proveedor, note que la velocidad del internet mejor y puedo revisar los dispositivos conectados en busca de intrusos. También puedo visualizar errores de configuración de los dispositivos conectados para solucionarlos y evitarle daños (junto con dinero extra para su reparación)
Paola Estefany Vásquez Duarte	La seguridad de mi red puede ser vulnerada si no tomo medias de protección buenas y mi información filtrada si mi consentimiento.

VIII. CONCLUSIÓN

Los objetivos propuestos al inicio de este proyecto que era brindar una herramienta para los usuarios finales que puedan usar para la identificación de sus vulnerabilidades y así puedan reducir los riesgos a los que están expuestos, se cumplió exitosamente a través del desarrollo de un manual (ver anexos) que abarca varios tópicos (vulneración de red wifi, inventario de dispositivos conectados e identificación de vulnerabilidades de los dispositivos conectados a la red), también resolviendo las dudas que tenían los usuarios ya sea en la aplicación del manual o en la interpretación de los resultados, logrando crearles conciencia acerca de los riesgos que corren dentro de su propia red, para este fin los usuarios pudieron visualizar por ellos mismo los resultados.

Respecto a los resultados a nivel general, por parte de los hallazgos encontrados por la muestra poblacional, se denota un uso inadecuado de las herramientas de seguridad que provee cada dispositivo (como es el uso de las actualizaciones automáticas) las cuales permiten que los dispositivos conectados no solo a la red hogareña sino también a redes externas puedan ser utilizados por sus dueños sin correr riesgos que involucren la integridad de la información almacenada allí como su software instalado, también con respecto al acceso externo desde la red por medio de la red Wifi la correcta configuración de la encriptación y clave de acceso a la red hogareña, lo que permite evitar el ingreso a la red de personas no deseadas que puedan ya sea simplemente utilizar el servicio o en el peor de los casos el uso abusivo de la información que pasa a través de la red.

Y por parte de los usuarios, que estos no sabían (hasta antes de aplicado el manual) que podían sacar un inventario para ver que dispositivos estaban conectados a su red y así poder llevar un control de las conexiones activas a la red, que podían validar la fortaleza de su red Wifi ante un posible ataque de intrusión y poder verificar y solventar las vulnerabilidades que tienen sus dispositivos.

La mejor practica que se puede ejecutar para concientizar a los usuarios acerca de los temas de seguridad es enseñándoles y dándoles las herramientas necesarias para que puedan hacer sus

diagnósticos y con base a ello tengan como prioridad su seguridad ante la red, lo cual pueden aplicar a sus amigos o aplicarlo en sus lugares de trabajo para así bajar las tazas de ciberataques que se llevan a cabo diariamente y proteger así los activos más valiosos, logrando la educación del eslabón más débil (el usuario).

REFERENCIAS

[1] Kaspersky, «Kaspersky Lab Daily,» [En línea]. Available: https://www.kaspersky.es/blog/. [Último acceso: 27 05 2019].

[2] R. Tecnósfera, «El Tiempo,» 23 08 2017. [En línea]. Available: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/mas-de-la-mitad-de-los-hogares-en-colombia-cuenta-con-acceso-a-internet-122714. [Último acceso: 08 05 2019].

[3] G. Saldana, «Kaspersky Lab Daily,» 14 08 2018. [En línea]. Available: https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-ataques-ciberneticos-en-america-latina/13266/. [Último acceso: 08 05 2019].

[4] P. Security, «Panda Mediacenter,» 18 09 2018. [En línea]. Available: https://www.pandasecurity.com/spain/mediacenter/seguridad/iot-en-casa-segura/. [Último acceso: 08 05 2019].

[5] A. Margosis, «Microsoft Security Guidance Blog,» Microsoft, 24 04 2019. [En línea]. Available: https://blogs.technet.microsoft.com/secguide/2019/04/24/security-baseline-draft-for-windows-10-v1903-and-windows-server-v1903/. [Último acceso: 20 05 2019].

[6] P. Segarra, «20 Minutos,» 23 03 2018. [En línea]. Available: https://www.20minutos.es/noticia/3282046/0/ciberdelincuencia-virus-informatica-malware-ataque-wifi-wanacry-spam-web/. [Último acceso: 08 05 2019].

[7] NetSpot, «NetSpot,» [En línea]. Available: https://www.netspotapp.com/es/wifi-encryption-and-security.html. [Último acceso: 08 05 2019].

[8] D. Ojeda, «El Espectador,» 15 01 2109. [En línea]. Available: https://www.elespectador.com/tecnologia/cuidado-estos-son-los-ataques-informaticos-que-seran-protagonistas-en-2019-articulo-834202. [Último acceso: 08 05 2019].

[9] C. Angarita Pinzón y C. Guzmán Flórez, «Universidad Catolica de Colombia Repositorio Institucional,» 2017. [En línea]. Available: https://repository.ucatolica.edu.co/handle/10983/15321. [Último acceso: 20 05 2019].

[10] Avast, «Avast Blog,» 01 02 2019. [En línea]. Available: https://blog.avast.com/es/predicciones-para-2019-el-internet-de-las-cosas-vulnerables. [Último acceso: 21 05 2019].

[11] M. Hron, «Avast Blog,» 16 08 2018. [En línea]. Available: https://blog.avast.com/mqtt-vulnerabilities-hacking-smart-homes. [Último acceso: 21 05 2019].

[12] Kaspersky LAB, «Kaspersky LAB,» [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Último acceso: 09 05 2019].

[13] Kaspersky, «Kaspersky Online Help,» 04 09 2018. [En línea]. Available: https://help.kaspersky.com/kts/2017/es-MX/90.htm#o37813. [Último acceso: 13 05 2019].

[14] P. Security, «Panda,» [En línea]. Available: https://www.pandasecurity.com/es/security-info/glossary/. [Último acceso: 13 05 2019].

[15] L. W. d. Programador, «La Web del Programador,» [En línea]. Available: https://www.lawebdelprogramador.com/diccionario/1163-Sistema-Operativo.html. [Último acceso: 13 05 2019].

[16] Kaspersky, «Kaspersky Lab,» [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware. [Último acceso: 13 05 2019].

[17] Protafolio, «Portafolio,» 21 04 2017. [En línea]. Available: https://www.portafolio.co/tendencias/bitcoin-tendencia-u-oportunidad-505153. [Último acceso: 13 05 2019].

[18] PBS, «PBS New Hour,» 16 05 2017. [En línea]. Available: https://www.pbs.org/newshour/science/everything-need-know-wannacrypt-ransomware-attack. [Último acceso: 14 05 2019].

[19] ccm, «es-ccm.net,» [En línea]. Available: https://es.ccm.net/faq/4321-cual-es-el-mejor-antispyware-gratuito. [Último acceso: 15 05 2019].

[20] I. N. d. Ciberseguridad, «Instituto Nacional de Ciberseguridad,» 20 02 2017. [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf. [Último acceso: 15 05 2019].

[21] AFP, «El tiempo.com,» 15 05 2019. [En línea]. Available: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/whatsapp-descubre-software-espia-para-atacar-a-usuarios-361288. [Último acceso: 15 05 2019].

[22] T. Sidorina , T. Shcherbakova y M. Vergelis, «Kaspersky Lab SecureList,» 15 05 2019. [En línea]. Available: https://securelist.lat/spam-and-phishing-in-q1-2019/88830/. [Último acceso: 23 05 2019].

[23] C. V. d. l. Policia, «Cai Virtual de la Policia,» [En línea]. Available: https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico. [Último acceso: 26 05 2019].

[24] G. LLC, «Google Maps,» 2019. [En línea]. Available: https://www.google.com/maps/@4.5439505,-74.0903501,335m/data=!3m1!1e3. [Último acceso: 24 08 2019].

[25] G. Martínez Atienza , «ebookcentral,» 01 01 2018. [En línea]. Available: https://ebookcentral.proquest.com/lib/biblioucatolicasp/detail.action?docID=5307732&query=ciberseguridad.

[26] P. Llaneza González , «ebookcentral,» 01 01 2018. [En línea]. Available: https://ebookcentral.proquest.com/lib/biblioucatolicasp/detail.action?docID=5636982&query=ciberseguridad.

[27] G. Escrivá Gascó, R. M. Romero Serrano y D. Jorge Ramada, «ebookcentral,» 01 01 2013. [En línea]. Available: https://ebookcentral.proquest.com/lib/biblioucatolicasp/detail.action?docID=3217398&query=malware.

[28] G. Álvarez Marañón y P. P. Pérez García, «ebookcentral,» 01 01 2004. [En línea]. Available: https://ebookcentral.proquest.com/lib/biblioucatolicasp/detail.action?docID=3195263&query=malware.

[29] F. Miró Llinares , «ebookcentral,» 01 01 2012. [En línea]. Available: https://ebookcentral.proquest.com/lib/biblioucatolicasp/detail.action?docID=5045441

&query=malware.

[30] J. L. González Cussac , «ebookcentral,» 01 01 2013. [En línea]. Available: https://ebookcentral.proquest.com/lib/biblioucatolicasp/detail.action?docID=3227368 &query=malware.

[31] J. Scambray y S. McClure , «ebookcentral,» 01 01 2009. [En línea]. Available: https://ebookcentral.proquest.com/lib/biblioucatolicasp/detail.action?docID=3191943 &query=malware.

[32] J. F. Roa Buendía, «ebookcentral,» 01 01 2013. [En línea]. Available: https://ebookcentral.proquest.com/lib/biblioucatolicasp/detail.action?docID=3211239 &query=malware.

[33] «Ciberseguridad afronta cambio de paradigma con grandes retos en Latinoamerica: LATINOAMÉRICA CIBERSEGURIDAD,» *EFE News Service; Madrid,* 15 11 2017.